НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Телекомунікаційних систем

«До захисту допущено»
Завідувач кафедри
_____ Леонід УРИВСЬКИЙ
«___»_____20__ р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності 172 Телекомунікації та радіотехніка

на тему: «Оцінка відповідності систем управління інформаційною безпекою автоматизованих систем управління технологічними процесами»

Виконав:
студент (-ка) IV курсу, групи ТС-72
Ковба Денис Ігорович _____

Керівник:
Професор кафедри ТС, д.т.н., професор
Горицький Віктор Михайлович _____

Рецензент:
Старший викладач СК 5 ІСЗЗІ КПІ
Мітін Сергій Вячеславович _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____

Київ – 2021 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Телекомунікаційних систем

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 Телекомунікації та радіотехніка»

Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____Леонід УРИВСЬКИЙ
«___»_____20__ р.

ЗАВДАННЯ
на дипломну роботу студенту
Ковбі Денису Ігоровичу

1. Тема роботи «Оцінка відповідності систем управління інформаційною безпекою автоматизованих систем управління технологічними процесами», керівник роботи Горицький Віктор Михайлович, професор, затверджені наказом по університету від «14» квітня 2021 р. №1007-с

2. Термін подання студентом роботи 9 червня 2021 року.

3. Вихідні дані до роботи: Інформаційні матеріали щодо оцінки відповідності систем управління інформаційною безпекою автоматизованих систем управління технологічними процесами. Структурований план порядку розробки матеріалів дипломної роботи.

4. Зміст роботи

Розглянути та проаналізувати структуру стандарів IEC 62443, розглянути системи управління інформаційною безпекою, стандартизацію забезпечення інформаційної безпеки, впровадження та сертифікації систем управління інформаційної безпеки IEC 62443 в Україні; розгляд основного органу з акредитації в Україні.

5. Перелік ілюстративного матеріалу (презентація, перелік слайдів): 1) Тема та цілі дипломної роботи; 2) Структура серії стандартів IEC 62443; 3) Рівні захисту у глибину; 4) Цикл PDCA для IEC 62443; 5) Життєвий цикл кібербезпеки; 6) Оцінка ризику; 7) Висновки по роботі

6. Дата видачі завдання: 13 квітня 2021 року

Календарний план

№	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Системи управління інформаційною безпекою. Їх місце в національній та глобальній інфраструктурі якості. Стандартизація систем управління інформаційною безпекою. Визначення інфраструктури якості.	19.04.2021	
2	Системи управління інформаційною безпекою на основі стандарту IEC 62443. Історія сімейства стандартів IEC 62443.Структура стандартів IEC 62443. Визначення рівнів зрілості.	22.05.2021	
3	Дослідження проблем впровадження та сертифікації систем управління інформаційною безпекою на основі IEC 62443. Національне агентство з акредитації. Впровадження стандарту IEC 62443 в Україні. Кібербезпека в Україні	30.05.2021	
6	Вступ, Висновки	06.06.2021	
7	Чистовий варіант дипломної роботи, плакати	08.06.2021	

Студент Денис КОВБА

Керівник роботи Віктор ГОРИЦЬКИЙ

АНОТАЦІЯ

Текстова частина дипломної роботи: 74 с., 15 рис.., 7 табл., 38 джерел.

Мета роботи: огляд систем управління інформаційної безпеки; огляд стандартів ISO/IEC 27001 та IEC 62443 і їх місце в глобальній інфраструктурі якості; розгляд стану кібербезпеки в Україні. В даній роботі проведено аналіз систем управління інформаційної безпеки в Україні та стан кібербезпеки. Впровадження стандартів IEC 62443 в Україні та порівняння з іншими країнами. Розглянуто закон України “Про сертифікацію”. Огляд ГОСТУ з приводу сертифікації.

ABSTRACT

The purpose of the work is to review of control system of informative safety; review of standards of ISO/IEC 27001 and IEC 62443 and their place in the global infrastructure of quality; consideration of the state of cybersecurity is in Ukraine.The analysis of control system of informative safety in Ukraine and state of кібербезпеки are conducted in this work. Introduction of standards of IEC 62443 in Ukraine and comparing to other countries. The law of Ukraine is considered "On a certification".

ЗМІСТ

ВСТУП

Окремим напрямком в забезпеченні кібербезпеки цифрової економіки України має стати, поряд з кібербезпекою IT-технологій, кібербезпека операційних технологій (OT- технологій), які стають основою для економіки 4.0. Операційні технології (OT), також відомі як системи промислової автоматизації та управління (IACS), промислові системи управління (ICS), розглядаються зараз як новий рубіж кібербезпеки.

Важливу роль в сфері кібербезпеки відіграє оцінка відповідності (сертифікація) кібербезпеки. Правила, процедури та менеджмент проведення сертифікації кібербезпеки встановлюють схему сертифікації, а набір правил та процедур для управління подібними або спорідненими схемами оцінки відповідності утворюють систему сертифікації. Створення схем сертифікації кібербезпеки ОТ на сьогодні є пріоритетним та актуальним. Зараз існує низка систем сертифікації, які можуть бути застосовані для сертифікації кібербезпеки ОТ, але вони не забезпечують взаємного визнання процедур і результатів випробувань і оцінок. Створення системи та схем сертифікації кібербезпеки на основі міжнародних та європейських принципів оцінки відповідності потребує відповідного наукового та методологічного забезпечення.

В роботі досліджується проблематика оцінки відповідності (сертифікації) систем управління інформаційною безпекою автоматизованих систем управління технологічними процесами (СУІБ ОТ).

Всі компанії на даний момент стикаються з кібербезпекою. Відповідно і з системою управління інформаційною безпекою. Перший стандарт із серії ISO/IEC 27001 системи управління інформаційною безпекою (СУІБ) був випущений більше 20 років тому, який задовільняв потреби користувачів. Але світ швидко розвивається і згодом з’явився стандарт IEC 62443.

IEC 62443, раніше відомий як ISA 99, є де-факто глобальним стандартом безпеки промислової системи управління (ICS). Стандарт був розроблений Міжнародним товариством автоматизації (ISA) та прийнятий Міжнародною

електротехнічною комісією (IEC), яка в даний час відповідає за його подальший розвиток.

Актуальність дипломної роботи полягає в дослідженні проблем оцінки відповідності систем управління інформаційною безпекою автоматизованих систем управління технологічними процесами в системі технічного регулювання України.

1 СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ. ЇХ МІСЦЕ В НАЦІОНАЛЬНІЙ ТА ГЛОБАЛЬНІЙ ІНФРАСТРУКТУРІ ЯКОСТІ

1.1 Інфраструктура якості

Головною метою національної політики у сфері нагляду за технологіями є забезпечення високого ступеня захисту громадян України як права споживачів надати безпечні та якісні товари (роботи, послуги) в умовах вільного вибору та сприяти вільному рух товарів у країні та на світовому ринку. Термін "технічне регулювання" все частіше з'являється в літературі та засобах масової інформації, і його значення до останнього часу не визначалося виразом "стандартизація та пов'язана з цим діяльність". Це відображає сучасну практику застосування нормативних документів (НД) та процедур оцінки відповідності, які базуються на обов'язкових вимогах технічних регламентів та інших добровільних вимогах НД.

Ці принципи покладені в основу документів Міжнародної організації з стандартизації, Світової організації торгівлі (СОТ) та Європейського Союзу (ЄС).

Створення Європейського Союзу базується на чотирьох основних принципах, а саме на "чотирьох свободах".

До них належать: вільний рух товарів, послуг, капіталу та людей. У минулому відмінності між національним законодавством, стандартами та процедурами оцінки відповідності ускладнювали торгівлю між країнами-членами ЄС важкою, дорогою та трудомісткою.

Потрібні більш швидкі дії, і всі торгові бар'єри між країнами-членами ЄС повинні бути усунені.

З метою прискорення усунення цих перешкод були запроваджені нові законодавчі методи та стратегії:

Новий метод (1985) та глобальний метод (1989).

Національна політика у галузі регулювання технологій спрямована на реформування національної системи на основі міжнародної та європейської практики. 13 липня 2005 р. Президент України оприлюднив Указ № 1105 "Заходи щодо вдосконалення діяльності у сфері регулювання технологій та споживчої

політики", який передбачає проведення реформ у цій галузі протягом 2006-2010 років.

Основними елементами системи технічних регламентів, що встановлена в Україні, є: закони; технічні регламенти; національні стандарти, що відповідають міжнародним та європейським вимогам; процедури оцінки відповідності; і нагляд за дотриманням обов'язкових вимог.

У Радянському Союзі держава несе повну відповідальність за безпеку продукції та послуг, а стандарти є законами. Нормативні документи суворо регламентують продукцію навіть для невеликих вимог, і всі вони повністю контролюються. Цей підхід не відповідає міжнародним нормам і правилам. Принципи СОТ, а саме Угода про технічні бар'єри в торгівлі, не сприяли впровадженню нових технологій та інновацій, і його постійно критикували торгові партнери України.

Реформування національної системи технічного регулювання почалося з прийняття в 2001 р. законів України «Про стандартизацію» № 2408-III від 17.05.2005 р. і «Про підтвердження відповідності» №2406-III від 17.05.2001 р., які відповідають принципам технічного регулювання, що діють в ЄС.

Основні принципи, впроваджені в законодавстві України про нові технології:

• Запровадити добровільне застосування стандартів;

• Пріоритетне безпосереднє впровадження міжнародних та європейських стандартів;

• Гармонізувати національні правила для підтвердження відповідності міжнародним та європейським стандартам;

• Застосування методу підтвердження відповідності залежить від потенційних ризиків, що відповідають міжнародній практиці, особливо декларації виробника про відповідність;

• Переконайтесь, що особа підтверджується відповідно до процедур вітчизняних та іноземних джерел;

• Створити незалежний орган із сертифікації для застосування стандартів, що відповідають міжнародним та європейським стандартам у галузі сертифікації.

Зокрема, український Закон про стандартизацію (стаття 12) містить основний принцип міжнародної стандартизації - добровільне застосування стандартів. Однак ці стандарти стануть добровільними лише після того, як обов'язкові вимоги безпеки для життя та здоров'я людей та вимоги щодо охорони навколишнього середовища будуть перетворені на технічні регламенти.

Стандарти, засновані на міжнародних нормах, повинні: слугувати основою для впровадження технічних регламентів та процедур оцінки відповідності продукції вимогам технічних регламентів; включати вдосконалені вимоги до якості та безпеки продукції; впроваджувати інноваційні досягнення та новітні технології в галузі якості та безпеки продукції. Найбільш складний процес вимагає участі великої кількості фінансових ресурсів, тобто запровадження прийнятих технічних регламентів для підтвердження відповідності та узгодження існуючих національних та міжнародних стандартів.

Закон України "Про стандарти оцінки відповідності, технічні регламенти та процедури" 7 1 грудня 2005 року Верховна Рада України прийняла український Закон "Про стандарти оцінки відповідності, технічні регламенти та процедури" [3164-IV. Розглянемо основні положення цього закону. Прийняті закони передбачають правову та організаційну основу для формування та застосування національних стандартів, технічних регламентів та процедур оцінки відповідності, а також основні принципи національної політики у галузі стандартизації, технічних регламентів та оцінки відповідності.

Перша частина - "Загальні положення" - конкретно визначає такі терміни:

• Призначення - Орган, призначений або уповноважений Кабінетом Міністрів України, надає органу з оцінки відповідності право виконувати певні заходи з оцінки відповідності технічним регламентам.

• Оцінка відповідності - щоб довести, що встановлені вимоги до продукції, процесів, систем, персоналу чи установ були виконані шляхом випробувань, інспекцій або сертифікації. Сфера оцінки відповідності включає такі види діяльності, як випробування, контроль та сертифікація, а також акредитацію органів з оцінки відповідності. Поняття "товар" включає поняття "послуга".

• Підтвердження відповідності - видача документів (декларація про відповідність або сертифікат відповідності) на основі рішень, прийнятих після відповідних (необхідних) процедур оцінки відповідності, які підтвердили відповідність встановленим вимогам.

• Процедура оцінки відповідності - будь-яка процедура, що використовується прямо чи опосередковано для визначення, чи виконуються вимоги, зазначені у відповідних технічних регламентах або стандартах. Процедури оцінки відповідності включають відбір зразків, випробування, перевірку, оцінку, перевірку, реєстрацію, акредитацію та затвердження та їх поєднання.

• Нагляд за ринком - постійний нагляд за дотриманням оборотної продукції, технічних регламентів, законністю застосування національних знаків відповідності, а також повнотою та точністю такої інформації про товар.

• Технічний регламент - українське законодавство або нормативно-правовий акт, прийнятий українським кабінетом, який визначає характеристики продукції або пов'язаних з нею процесів чи методів виробництва, а також вимоги до послуг, що включають відповідні нормативні акти. 8 пунктів повинні відповідати цим правилам. Він також може містити вимоги до термінології, маркування, упаковки, маркування або маркування, що застосовуються до певного продукту, процесу або способу виробництва.

• Технічні регламенти-закони та нормативні акти, пов'язані із встановленням, застосуванням та впровадженням обов'язкових вимог до продуктів або пов'язаних із ними процесів, систем та послуг, персоналу та установ та перевірки їх відповідності шляхом оцінки відповідності та / або нагляду за ринком.

Перша частина також містить загальні принципи щодо формулювання та застосування стандартів, технічних регламентів та процедур оцінки відповідності.

Друга частина закону - "Процедури формування та прийняття стандартів" - передбачає процедури формулювання стандартизації, формулювання та прийняття національних стандартів та їх перегляду, внесення змін та скасування робочих планів.

Третя частина - "Технічний регламент" - сформулювала мету та національну політику в галузі технічних регламентів. Необхідно наголосити на тому, що щодо продуктів, процесів та послуг, що циркулюють в Україні, повинні виконуватися вимоги технічних регламентів. Цей розділ визначає повноваження Кабінету Міністрів України, центрального органу виконавчої влади з питань нагляду за технологіями та інших відомств, що працюють у цій галузі. Наведені процедури формулювання, прийняття та перегляду технічних регламентів.

Проекти технічних регламентів зазвичай повинні включати:

• Технічні вимоги до продуктів, процесів або послуг, що відповідають рівню науки і техніки, досягнутим під час розробки, включаючи безпеку;

• Процедури оцінки відповідності, які можна або повинні використовувати для перевірки відповідності продукції технічним вимогам;

• Вимоги до упаковки, вміст етикетки товару, технічні характеристики (за необхідності) - важлива інформація про споживача (інструкції, посібники), яка вводиться в обіг із товаром або процесом.

Якщо проект технічного регламенту передбачає можливість декларації про відповідність, він повинен включати процедуру декларування, форму, зміст та термін зберігання декларації про відповідність.

У четвертому розділі - "Процедури оцінки відповідності Технічним регламентам" - Цей закон визначає вимоги та відповідальність органів з оцінки відповідності, а також процедури визнання результатів оцінки відповідності, проведених за межами України. 9 Слід зазначити, що виробник повинен підготувати декларацію про відповідність для всіх товарів, що вводяться в обіг, що відповідають вимогам технічних регламентів, якщо технічний регламент не передбачає іншого.

Якщо технічним регламентом не передбачено інше, декларація про відповідність повинна містити таку інформацію:

• Ідентифікація продукту (назва, тип або модель, будь-яка додаткова інформація, така як номер партії або серійний номер, назва компонента);

• Технічні та нормативні вимоги, яким відповідає виріб, включаючи посилання на відповідні національні стандарти;

• Додаткова інформація відповідно до технічних регламентів (різновид або категорія продукції);

• Дата реєстрації, ім'я, адреса, статус та підпис виробника або його уповноваженого представника;

• Назва, адреса та ідентифікаційний код у реєстрі уповноваженого органу органу з оцінки відповідності, що виконує процедуру оцінки відповідності;

• Зберігайте назву та адресу технічного документа про підтвердження відповідності.

Виробник повинен отримати сертифікат відповідності від органу з оцінки відповідності відповідно до законодавчих вимог, якщо така процедура зазначена в технічному регламенті, для підтвердження відповідності. Форма декларації про відповідність визначається центральним органом виконавчої влади з оцінки відповідності. Кабінет Міністрів України визначає зразки (інструкції) та затверджує правила застосування національного знака відповідності для підтвердження відповідності технічним регламентам.

Розділ п’ятий - "Зобов'язання виробників та постачальників продукції, що підпадають під дію Технічного регламенту, та контроль за дотриманням технічних регламентів" - передбачає, що виробники та постачальники повинні забезпечити відповідність відповідним технологіям перед введенням технічних регламентів. Усі вимоги регламенту. Технічний регламент. Якщо відповідні технічні регламенти мають положення, введення його в обіг супроводжуватиметься декларацією про відповідність та / або сертифікатом відповідності, а також знаком товару з національним знаком відповідності. Фундаментальною новою концепцією закону є концепція ринкового нагляду. Варто зазначити, що метою нагляду за ринком є контроль за тим, чи імпортується продукція, процеси та послуги відповідають вимогам технічних регламентів щодо безпеки та здоров’я тварин, тварин, рослин, навколишнього середовища та природних ресурсів, запобігання несправедливій практиці, та забезпечити справедливість. 10 цілей конкуренції для підприємницької діяльності. Нагляд за ринком здійснюється адміністративними органами відповідно до законодавства.

Розділ VI - "Надання інформації про технічні регламенти, стандарти та процедури оцінки відповідності" - передбачає створення Центру обробки запитів Кабінету Міністрів України та повідомлення про стандарти, технічні регламенти та процедури оцінки відповідності, який визначає функціональні центри України. Центральний орган виконавчої влади, що розробляє стандарти, технічні регламенти та процедури оцінки відповідності, повинен подати копії цих документів до призначеного центру протягом п’яти робочих днів після того, як проекти документів будуть завершені.

У сьомій частині - "Прикінцеві положення" - в українські закони "Про оцінку відповідності" та "Про стандартизацію" було внесено деякі зміни, що стосуються термінології, цілей та завдань стандартизації, стандартизації функцій центрального органу виконавчої влади та застосування стандартів. Ці стандарти застосовуються на добровільних засадах, якщо це не вимагається технічними регламентами. Процедури формулювання, перегляду, перегляду та прийняття стандартів регулюються розглянутим українським законом "Про стандарти, технічні регламенти та процедури оцінки відповідності".

Об'єктивно кажучи, з появою інформаційно-комунікаційних методів між людьми, і люди усвідомлюють, що існування людей в людях та їх інтересах спільнот може забезпечити та налагодити взаємозв'язок між усіма елементами суспільства завдяки інформаційному спілкуванню, існуванню та його розвитку Обмін інформацією.

З огляду на вплив зміни мислення інформаційної безпеки на інформаційну безпеку, розвиток інформаційного спілкування можна розділити на кілька етапів:

Перший етап - до 1816 р. - характеризується використанням природних методів обміну інформацією. Протягом цього періоду головним завданням інформаційної безпеки є захист інформації про події, факти, властивості, місцезнаходження та інші дані, які є життєво важливими для окремих людей чи їхніх спільнот.

Другий етап - починаючи з 1816 р. - пов’язаний з початком використання штучно створених телекомунікаційних та радіотехнологій. Для забезпечення

конфіденційності та захищеності від шуму радіозв'язку необхідно використовувати досвід захисту інформації на першому етапі на найвищому технічному рівні, тобто використовувати шумостійке кодування повідомлення (сигналу), а потім декодувати інформація. Повідомлення (сигнал) отримано.

Третій етап - з 1935 року - пов’язаний з появою радарів та гідролокаторів. У цей період основним способом забезпечення інформаційної безпеки є поєднання організаційно-технічних заходів, спрямованих на вдосконалення захисту радарів від впливу їх приймального обладнання за допомогою активного маскування та пасивного моделювання електронних перешкод.

Четвертий етап - з 1946 р. - пов'язаний з винаходом та реалізацією практичних комп'ютерів (комп'ютерів). Завдання інформаційної безпеки в основному вирішується методами та методами, що обмежують фізичний доступ до обладнання для вилучення, обробки та передачі інформації.

П’ятий етап, починаючи з 1965 року, обумовлений створенням та розвитком місцевих інформаційно-комунікаційних мереж. Завдання інформаційної безпеки також вирішено, головним чином, за допомогою методів та методів фізичного захисту засобів вилучення, обробки та передачі інформації, а також уніфікованого управління та управління доступом до мережевих ресурсів у локальній мережі.

Шостий етап, починаючи з 1973 року, передбачає використання пристроїв мобільного зв'язку із широким колом завдань. Загроза інформаційній безпеці стала більш серйозною. Для забезпечення інформаційної безпеки комп’ютерних систем з бездротовими мережами передачі даних необхідно сформулювати нові стандарти безпеки. Сформовано хакерське співтовариство, метою якого є підрив інформаційної безпеки окремих користувачів, організацій та всієї країни. Інформаційні ресурси стали найважливішим ресурсом країни, що забезпечує національну безпеку - найважливішою та обов'язковою складовою національної безпеки. Інформаційне право формується - нова галузь міжнародно-правової системи.

Сьомий етап - з 1985 року - пов’язаний зі створенням та розвитком глобальних інформаційно-комунікаційних мереж, що використовують космічні

активи. Можна припустити, що наступний етап розвитку інформаційної безпеки, очевидно, буде пов’язаний із широким використанням мобільних комунікаційних пристроїв, які мають широкий спектр завдань та глобальний простір-час, що забезпечується просторовими інформаційно-комунікаційними системами. Для вирішення поточних питань інформаційної безпеки необхідно побудувати макросистему інформаційної безпеки людини під егідою провідних міжнародних форумів.

З розвитком нових IT-технологій концепція інформаційної безпеки була значно розширена. Деякі експерти зазначали, що доцільніше повністю замінити поняття інформаційної безпеки поняттям мережевої безпеки. Це тому, що в наш час ми більше покладаємось на захист процесів, інформації та діяльності в кіберпросторі, а не лише на втрату інформації. Іншими словами, втрата інформації призведе до багатьох інших складних проблем. Безпека мережі - це захист від вірусів, хакерських атак та підробки даних. Зрештою, беручи для прикладу вірус, він може не тільки видаляти або красти дані, але й впливати на роботу та продуктивність працівників або навіть зупиняти виробництво. Інформація також може використовуватися проти людей або структур. Сьогоднішня кібербезпека відповідає за три фактори: системи, процеси та люди. Крім того, оскільки цифрові технології широко інтегровані у життя та тіло людини, питання інформаційної безпеки іноді стають проблемами безпеки життя. Тому стара концепція інформаційної безпеки не може дати відповіді на широке коло питань, що виникають у кіберпросторі у 21 столітті. Навпаки, інформаційна безпека перетворилася на частину мережевої безпеки.

1.2Система управління інформаційною безпекою (СУІБ)

Система управління інформаційною безпекою (СУІБ) є частиною загальної системи управління, заснованої на аналізі ризиків, призначеної для проектування, впровадження, контролю, моніторингу та вдосконалення діяльності з інформаційної безпеки. Система складається з організаційної структури, політики, запланованих

дій, відповідальності, процедур, процесів та ресурсів. Найважливішою метою більшості систем інформаційної безпеки є захист бізнесу та знань компанії від знищення або витоку. Крім того, однією з головних цілей системи захисту інформації є захист майнових прав споживачів. Водночас заходи інформаційної безпеки не повинні обмежувати або ускладнювати процес обміну інформацією всередині компанії, оскільки це може загрожувати розвитку організації.

Система управління інформаційною безпекою повинна забезпечити досягнення наступних цілей: забезпечення конфіденційності ключової інформації, забезпечення можливості несанкціонованого доступу до ключової інформації, цілісність інформації та пов'язаних із нею процесів (створення, введення, обробка та виведення) та деякі інші цілі. Досягнення поставлених цілей, швидше за все, дозволить вирішити такі основні завдання, як виявлення особи, відповідальної за інформаційну безпеку, формулювання ряду ризиків інформаційної безпеки та проведення експертних оцінок щодо них, формулювання політики та правил доступу до інформаційних ресурсів та формулювання систем управління ризиками інформаційної безпеки, включаючи їх методи оцінки та контролю Інформаційна безпека підприємства. Слід зазначити, що це далеко не повний перелік.

Побудова СУІБ дозволяє чітко визначити, як процеси та підсистеми ІС пов’язані між собою, хто за них відповідає, які фінансові та трудові ресурси потрібні для їх ефективної роботи тощо.

Основні функції системи управління інформаційною безпекою:

виявлення та аналіз ризиків інформаційної безпеки;

Планування та фактична реалізація процесів, спрямованих на мінімізацію ризиків інформаційної системи;

контролювати ці процеси;

Внести необхідні корективи в процес мінімізації інформаційного ризику.

Якісне управління інформаційною безпекою базується на таких принципах:

Комплексне управління інформаційно-підхідною системою повинно бути комплексним, що охоплює всі компоненти прав інтелектуальної власності та

враховує всі відповідні фактори ризику, що діють всередині та за межами інформаційної системи підприємства;

узгоджувати бізнес-цілі та стратегію компанії;

Високий ступінь контролю;

адекватність використаної та генерованої інформації;

Ефективність - найкращий баланс між можливостями, продуктивністю та вартістю СУІБ;

безперервність управління;

процесний підхід – пов’язати процес управління із замкнутим циклом планування, впровадження, перевірки, аудиту та коригування та підтримувати нерозривний зв’язок між різними етапами.

Одним із ключових факторів успіху корпоративної системи управління інформаційною безпекою є те, що вона базується на міжнародному стандарті ISO / IEC 27001.

1.3 Міжнародний стандарт ISO 27001

Міжнародний стандарт ISO 27001 забезпечує інструмент для розробки, впровадження, підтримання, моніторингу, підтримки та вдосконалення добре задокументованої системи управління інформаційною безпекою в контексті бізнес-ризиків.

СУІБ пропонує вибір відповідних та пропорційних методів та засобів для контролю та захисту інформації та довіри зацікавлених сторін.

Однак слід враховувати інші стандарти у галузі інформаційної безпеки. В даний час у міжнародній практиці використовується велика кількість стандартів, методів та інших документів, що регулюють процес управління інформаційною безпекою, таких як ISM3, COBIT, ITIL / ITSM, BSI-100-2, ISO13335-4, CRAMM, ISO15408. Але слід зазначити, що всі вони сумісні з ISO 27001 та подібними до нього.

У наш цифровий вік різні інформаційні технології розвиваються дуже швидко, але, на жаль, розвивається і кіберзлочинність.

Ключовим аспектом запобігання кіберзлочинності є підготовка та виявлення вразливих місць, а також гнучкість у взаємодії зі спільними системами управління. Серія стандартів ISO / IEC 27000, розроблена Спільним технічним комітетом Міжнародної організації зі стандартизації (ISO) та Міжнародною електротехнічною комісією (IEC) -ISO / IEC JTC 1, допоможе керувати інформаційною безпекою, а також виявити злочинців та їх до справедливості.

Перший стандарт із серії ISO / IEC 27001 Система управління інформаційною безпекою (СУІБ) був випущений більше 20 років тому. З тих пір серія опублікувала понад 40 міжнародних стандартів, що охоплюють все: від створення спільного словника (ISO / IEC 27000), управління ризиками (ISO / IEC 27005), безпеки хмарних технологій (ISO / IEC 27017 та ISO / IEC 27018) Криміналістичні методи аналізу цифрових доказів та розслідування подій (ISO / IEC 27042 та ISO / IEC 27043).

Наприклад, ISO / IEC 27043 містить керівні принципи, що описують процеси та принципи, що застосовуються до різних типів досліджень, включаючи несанкціонований доступ, пошкодження даних, збої в системі або порушення корпоративної інформаційної безпеки, а також будь-які інші дані цифрового опитування.

Виробники стандартів серії ISO / IEC 27000 помітили, що основні стандарти серії ISO / IEC 27001 постійно вдосконалюються, що дозволяє підприємствам постійно оновлюватись у боротьбі з кіберзлочинністю. Впроваджуючи ISO / IEC 27001, організації можуть оцінювати свої ризики, впроваджувати засоби контролю за зменшенням наслідків, потім відстежувати та переглядати свої ризики та контролювати їх, а також покращувати захист за потреби. Тому вона готова напасти в будь-який час.

Система управління інформаційною безпекою ISMS застосовується до всіх типів організацій та всіх видів підприємницької діяльності, включаючи малі та середні підприємства (МСП) як частину ланцюга поставок, тому важливо, щоб вони

контролювали та управляли своєю інформаційною безпекою та кібер ризикує захистити себе та інших.

І нещодавно був сформульований новий стандарт у галузі інформаційної безпеки-ISO / IEC 27552 "метод захисту". Розширте ISO / IEC 27001 та ISO / IEC 27002 для управління приватною інформацією. Вимоги та керівні принципи "додатково розширює ISO / IEC 27001 для вирішення конкретних вимог конфіденційності. В даний час на етапі проекту цей документ визначає вимоги та містить вказівки щодо підтримання та постійного вдосконалення управління конфіденційністю в організаційному середовищі.

Отже, серія стандартів ISO / IEC 27000 допомагає зробити всі сфери інформаційного життя більш захищеними, захистити конфіденційність, фінанси, особисту чи корпоративну репутацію та одночасно продовжувати розвиватися та вдосконалюватися.

1.4 Стандартизація підходів до забезпечення інформаційної безпеки

Без розуміння відповідних стандартів та норм сьогодні експертам у галузі ІС практично неможливо. Для цього є кілька вагомих причин. Формальною причиною є те, що законодавство вимагає певних стандартів (наприклад, документи щодо шифрування та інструкції від Федерального управління з питань технологій та експорту). Переконливі та змістовні причини. Перш за все, стандарти та специфікації - це форма накопичення знань, головним чином пов’язана з процедурами ІС та ІС та рівнями програмних технологій. Вони документують перевірені високоякісні рішення та методи, розроблені найбільш кваліфікованими компаніями у галузі розробки програмного забезпечення та забезпечення програмного забезпечення. По-друге, обидва є основними засобами забезпечення взаємодії апаратних та програмних систем та їх компонентів.У Інтернет-спільноті цей інструмент є дуже ефективним.

На верхньому рівні ми можемо розрізнити два абсолютно різних стандарти та технічні характеристики:

1) Стандарти оцінки, призначені для оцінки та класифікації інтелектуальної власності та заходів безпеки;

2) Регулювати всі аспекти впровадження та використання засобів і методів захисту.

Ці групи доповнюють одна одну. Стандарт оцінки описує найважливіші концепції та аспекти ІБ з точки зору ІС та виконує роль специфікації організації та структури. Спеціалізовані стандарти та специфікації точно визначають, як побудувати ІС пропонованої архітектури та відповідати організаційним вимогам.

Оцінка включає стандарт Міністерства оборони США "Стандарти оцінки надійних комп'ютерних систем" та його інтерпретацію конфігурації мережі, "Європейські національні гармонізовані стандарти", Міжнародні стандарти "Стандарти оцінки інформаційної безпеки", і звичайно Рекомендації Федеральної служби, технології та контроль експорту. До цієї ж групи входить Федеральний стандарт США "Вимоги безпеки до криптографічних модулів", який визначає конкретний, але дуже важливий і складний аспект інформаційної безпеки.

Технічні специфікації, що застосовуються до сучасних розподілених ІС, в основному створюються робочою групою з питань Інтернет-інженерії (IETF) та її робочою групою з питань безпеки. Ядром технічної специфікації є документ про рівень захисту IP (IPsec). Крім того, аналізуються захист на транспортному рівні (TLS) та захист на рівні програми (специфікація GSS-API, Kerberos). Інтернет-спільнота приділила належну увагу управлінню безпекою та процедурам, а також створила низку посібників та рекомендацій: "Керівні принципи інформаційної безпеки", "Як вибрати постачальників послуг Інтернету", "Як боротися з порушеннями інформаційної безпеки" тощо.

Що стосується мережевої безпеки, H.800 "Архітектура інтерактивної безпеки відкритої системи", H.500 "Служба каталогів: Огляд, концепція, модель та послуга" та H.509 "Служба каталогів: відкритий ключ та система сертифікатів атрибутів" нероздільні.

Стандарти оцінки механізмів захисту програмних технологій запропоновані у міжнародному стандарті ISO 15408-1999 "Загальні стандарти оцінки безпеки

інформаційних технологій", а "Загальні стандарти", прийняті в 1999 році, визначають функціональні вимоги до безпеки та вимоги до забезпечення безпеки.

"Загальний стандарт" містить два основні типи вимог безпеки:

1) Функція, яка відповідає активному аспекту захисту, подається функції захисту (служби) і реалізує її механізм;

2) Пасивні аспекти відповідають вимогам довіри; вони знайомляться з технологією та процесом розробки та експлуатації.

Розробити вимоги до безпеки та перевірити їх реалізацію щодо конкретних об’єктів оцінки (апаратних та програмних продуктів або IP). "ОК" в безпеці розглядається не статично, а відповідно до життєвого циклу об'єкта оцінки. Крім того, об’єкт, що перевіряється, з’являється не ізольовано, а у „безпечному середовищі”, яке характеризується певними лазівками та загрозами. "Загальні стандарти" слід використовувати для оцінки рівня безпеки на основі цілісності функцій безпеки, реалізованих у них, та надійності реалізації цих функцій. Хоча застосовність "ОК" обмежена програмними та апаратними механізмами захисту, вони включають набір механізмів захисту на рівні організації та вимог до фізичного захисту, які безпосередньо пов'язані з описаними функціями безпеки.

Британський стандарт BS 7799 "Практичні правила управління інформаційною безпекою" скопійований з міжнародного стандарту ISO / IEC 17799-2005 "Практичні правила управління інформаційною безпекою" ("Кодекс практики управління інформаційною безпекою") без особливих змін. Цей стандарт узагальнює правила та управління ІБ, які можуть бути використані як стандарти для оцінки організаційних механізмів безпеки, включаючи управління, процедури та заходи фізичного захисту.

Практичні правила розділені на 10 частин.

1. Політика безпеки.

2. Організаційний захист.

3. Класифікація та контроль ресурсів.

4. Безпека працівника.

5. Особиста безпека.

6. Комп’ютерна система та управління мережею.

7. Контроль доступу.

8. Розробка та обслуговування інформаційних систем.

9. Сплануйте безперебійну роботу організації.

10. Стежити за дотриманням вимог політики безпеки.

Ці розділи описують механізми на рівні організації, які в даний час застосовуються в державних та ділових організаціях багатьох країн.

Ключові інструменти управління (механізм управління ІБ), запропоновані у ISO 17799-2005, вважаються особливо важливими. Деякі засоби контролю (наприклад, шифрування) можуть вимагати поради та оцінки ризиків експертів з безпеки. У деяких випадках може знадобитися посилений контроль за ISO 17799-2005 для захисту особливо цінних ресурсів або реагування на особливо серйозні загрози безпеці. Процедура аудиту безпеки IP 17799 включає перевірку наявності перелічених ключових заходів контролю, оцінку повноти та правильності їх виконання та аналіз того, чи адекватно вони справляються з ризиками в робочому середовищі. Аналіз та управління ризиками також є частиною аудиторської роботи.

У 2005 році на основі версії ISO 17799-2000 було сформульовано стандарт інформаційної безпеки ISO / IEC 27002-2005 "Інформаційні технології. Технології безпеки. Практичні правила управління інформаційною безпекою" (Information technology. Security techniques. Code of practice for information security management). Стандарт описує найкращі практики управління інформаційною безпекою, які в стандарті визначаються як "збереження конфіденційності (вважаючи, що інформація доступна лише тим, хто має такі права доступу), цілісність (гарантування точності та повноти інформації та методів) Секс "). Обробка) та доступність (забезпечити доступ уповноважених користувачів до інформації та відповідних ресурсів) ".

Поточна версія стандарту зберігає структуру попередньої версії та дещо розширює її. Стандарт складається з наступних основних частин.

1. Політика безпеки.

2. Організація інформаційної безпеки.

3. Управління активами.

4. Гарантія людських ресурсів.

5. Фізична та екологічна безпека.

6. Зв'язок та управління експлуатацією.

7. Контроль доступу.

8. Придбання, розробка та обслуговування системи (придбання, розробка та обслуговування інформаційної системи).

9. Управління інцидентами інформаційної безпеки.

10. Управління безперервністю бізнесу.

11. Дотримання нормативних вимог (Відповідність).

Стан стандарту ISO / IEC 27005-2008 (BS 7799-3: 2006) "Настанови щодо управління ризиками інформаційної безпеки" тепер доступний.

Перелік російських стандартів у галузі інформаційної безпеки, заснований на відповідних міжнародних стандартах, включає:

o ГОСТ Р 50922-2006 "Захист інформації. Основні терміни та визначення";

o ГОСТ Р 51188-98 "Захист інформації. Випробування програмних засобів на наявність комп'ютерних вірусів. Типове керівництво";

o ГОСТ Р 51275-2006 "Захист інформації. Об'єкт інформатизації. Фактори, що впливають на інформацію. Загальні положення";

o ГОСТ Р ІСО/МЕК 15408-1-2008 "Інформаційна технологія. Методи та засоби забезпечення безпеки. Критерії оцінки безпеки інформаційних технологій. Частина 1. Введення і загальна модель";

o ГОСТ Р ІСО/МЕК 15408-2-2008 "Інформаційна технологія. Методи та засоби забезпечення безпеки. Критерії оцінки безпеки інформаційних технологій. Частина 2. Функціональні вимоги безпеки";

o ГОСТ Р ІСО/МЕК 15408-3-2008 "Інформаційна технологія. Методи та засоби забезпечення безпеки. Критерії оцінки безпеки інформаційних технологій. Частина 3. Вимоги довіри до безпеки";

o ГОСТ Р 50.1.053-2008 "Інформаційні технології. Основні терміни і визначення в галузі технічного захисту інформації";

o ГОСТ Р ІСО/МЕК 15408-2008 "Інформаційна технологія. Методи та засоби забезпечення безпеки. Загальні критерії оцінки безпеки інформаційних технологій".

У стандарті визначено інструменти та методика оцінки безпеки інформаційних продуктів і систем. Він містить перелік вимог, за якими можна порівнювати результати незалежних оцінок безпеки, завдяки чому споживач приймає рішення про безпеку продуктів. Сфера застосування цього стандарту - захист інформації від НСД, модифікації чи витоку та інші способи захисту, реалізовані апаратними та програмними засобами;

о ГОСТ Р ІСО/МЕК 17799-2005 "Інформаційні технології. Практичні правила управління безпекою інформації". Пряме застосування міжнародного стандарту з доповненням - ISO/IEC 17799:2005;

о ГОСТ Р ІСО/МЕК 27001-2006 "Інформаційні технології. Методи безпеки. Система управління безпекою інформації. Вимоги". Пряме застосування міжнародного стандарту - ISO/IFX 27001:2005;

о ГОСТ Р 51898-2002 "Аспекти безпеки. Правила включення в стандарти".

На нижньому рівні розроблені в різних країнах сотні галузевих стандартів, нормативних документів і специфікацій щодо забезпечення ІБ, які застосовуються національними компаніями при розробці програмних засобів, ІС та забезпечення якості і безпеки їх функціонування.

1.5 Висновки до розділу 1

Головною метою є впровадження міжнародних стандартів в Україні. Система управління інформаційною безпекою пропонує вибір відповідних та пропорційних методів та засобів для контролю та захисту інформації та довіри зацікавлених сторін. Ключовим аспектом кібербезпеки є серія сертифікатів ISO 2700. Вони допомагають знайти вразливі місця в системі.

2 СИСТЕМИ МЕНЕДЖМЕНТУ(УПРАВЛІННЯ) ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОСНОВІ СТАНДАРТУ IEC 62443

Всі експерти в області ІБ погоджуються, що забезпечення безпеки АСУ ТП відрізняється від забезпечення безпеки корпоративних інформаційних систем (далі КІС). Навіть сам термін "інформаційна безпека", настільки звичний ІТ-фахівцям, як правило, не застосовується до АСУ ТП. В першу чергу це пов'язано з тим, що необхідно приділяти увагу не тільки і не стільки забезпечення конфіденційності, скільки забезпечення безперервності і цілісності самого технологічного процесу. Більш того, безпеку технологічного процесу в загальному сенсі - це перш за все безпека для життя і здоров'я людей і навколишнього середовища. В англомовних джерелах для визначення "комп'ютерної безпеки" щодо АСУ ТП використовується спеціальний термін - cybersecurity (кібербезпека). У наших же реаліях спостерігається явний пробіл не тільки в нормативній та методичної бази в галузі забезпечення безпеки АСУ ТП, але навіть в термінології.

Для успішної реалізації проектів із захисту АСУ ТП необхідно використовувати підхід, заснований на об'єднанні існуючих (і розроблюваних) вимог регуляторів, з одного боку, і кращих світових практик - з іншого. Одним з основних наборів міжнародних методичних документів щодо забезпечення кібербезпеки АСУ ТП є сімейство стандартів IEC 62443 (раніше відоме як ISA 99). Про нього і піде мова в цій статті.

2.1 Стандарти IEC 62443

Стандарти IEC 62443 пропонують сучасний ризик-орієнтований підхід: безпека розглядається як сукупність безперервних процесів, які необхідно підтримувати на всіх стадіях життєвого циклу системи. Стандарти IEC 62443 задають вимоги до проектування накладених систем управління кібербезпекою АСУ ТП і SCADA і до проектування АСУ ТП з уже закладеними і інтегрованими заходами безпеки.

Загальний підхід до державотворчих процесів системи управління кібербезпекою АСУ ТП, аналізу та управління ризиками частково схожий з аналогічним, заданим стандартом ISO 27001 для IT-систем. Основою для визначення вимог, що пред'являються до проектованої системі, є аналіз ризиків. Наріжними каменями аналізу ризиків є ідентифікація, класифікація та оцінка. Начебто все знайоме, але диявол криється в деталях - схожість з відомими для IT-фахівців практиками полягає в тому, що треба зробити. А ось те, як це треба робити, істотно відрізняється.

Вибір методики оцінки ризиків залишається на розсуд власника АСУ ТП і залежить від специфіки використовуваних систем. Втім, загальні рекомендації в стандарті описані. Ми в своїй роботі використовуємо власну методику аналізу ризиків, адаптовану під конкретний об'єкт захисту, що задовольняє вимогам кращих практик, з одного боку, і відповідає російським нормативним документам - з іншого.

Для більшості систем АСУ ТП найбільш важливою є так звана HSE-група наслідків, що призводять до збитку здоров'ю або безпеці людей і навколишнього середовища (Health, Safety and Environmental), а також введені проектом нормативних документів ФСТЕК "наслідки в соціальній, політичній, економічній, військовій чи інших областях діяльності "(для простоти будемо називати їх ПЕВ).

На початку робіт зі створення системи управління кібербезпекою АСУ ТП проводиться високорівнева оцінка ризиків, покликана визначити основні фінансові, ПЕВ- і HSE-наслідки в разі порушення доступності, цілісності або конфіденційності. Високорівнева оцінка дає уявлення про загальну картину ризиків і критичних систем і є базисом для переходу до більш детального вивчення об'єкта, що захищається.

Наступним кроком при створенні системи управління кібербезпекою є аналіз об'єкта захисту, ідентифікація і класифікація активів АСУ ТП, які підлягають захисту. Спробуємо коротко висвітлити підхід, що описується в IEC 62443.

IEC 62443, раніше відомий як ISA 99, є де-факто глобальним стандартом безпеки промислової системи управління (ICS). Стандарт був розроблений Міжнародним товариством автоматизації (ISA) та прийнятий Міжнародною

електротехнічною комісією (IEC), яка в даний час відповідає за його подальший розвиток. ISA 99 та TC65 робочий комітет IEC 10 (TC65WG10) спільно розробили низку нормативних документів IEC 62443 для задоволення потреб впровадження мережевої безпеки та стійкості в системах промислової автоматизації. ISA99 / IEC 62443 пов'язаний з безпекою промислових систем управління та є більш широко відомим як "промислова автоматизація та системи управління". Метою цієї серії стандартів є забезпечення того, щоб постачальники продукції, інтегратори та власники активів виконували ефективні процеси. Ключові аспекти - це безпека персоналу та виробництва, наявність, ефективність та якість продукції IACS, а також екологічна безпека. Метою серії IEC 62443 є підвищення функціональної безпеки, доступності, цілісності та конфіденційності компонентів або систем, що використовуються в промисловій автоматизації, включаючи аспекти закупівель;

Серія IEC 62443 базується на існуючих загальних стандартах інформаційної безпеки системи інформаційних технологій (таких як серія ISO / IEC 27000). Основні відмінності полягають у наступному:

• Деякі інші аспекти функціональної безпеки, здоров'я та навколишнього середовища, які не пропонуються в ISO / IEC 27001 та ISO / IEC 27005);

• Існування деяких додаткових термінів та визначень.

Основною метою серії IEC 62443 є створення гнучкої структури, яка допомагає вирішити поточні та майбутні вразливості в системах промислової автоматизації, а також систематично та захисно застосовувати необхідні засоби пом'якшення наслідків.

Серія IEC 62443 призначена для підвищення корпоративної безпеки шляхом коригування вимог IT-систем бізнесу та їх поєднання з унікальними вимогами щодо доступності, що вимагаються системами промислової автоматизації.

Основними пунктами стандарту IEC 62443-2-1: 2010 є такі:

• Визначити елементи, необхідні для створення системи управління кібербезпекою (CSMS) для систем промислової автоматизації, та надати вказівки щодо її розвитку;

• Забезпечити структуру у формі політики та процедур для створення остаточної організації СМСС;

• охоплювати практики, пов’язані з працівниками;

• Підкресліть необхідність узгодження практики управління кібербезпекою в системах промислової автоматизації з практикою управління кібербезпекою в бізнес-системах та / або інформаційних технологіях.

2.2 Структура серії IEC 62443

У серії нормативних документів IEC 62443 є 14 документів, розділених на чотири рівні (див. рис 2.1):

• Загальний рівень.

• Рівень системи управління (політики та процедури), промислова IT-безпека.

• Рівень промислової автоматизації та управління системою IACS (системні вимоги) та безпека вбудованих систем.

• Рівень компонентів.

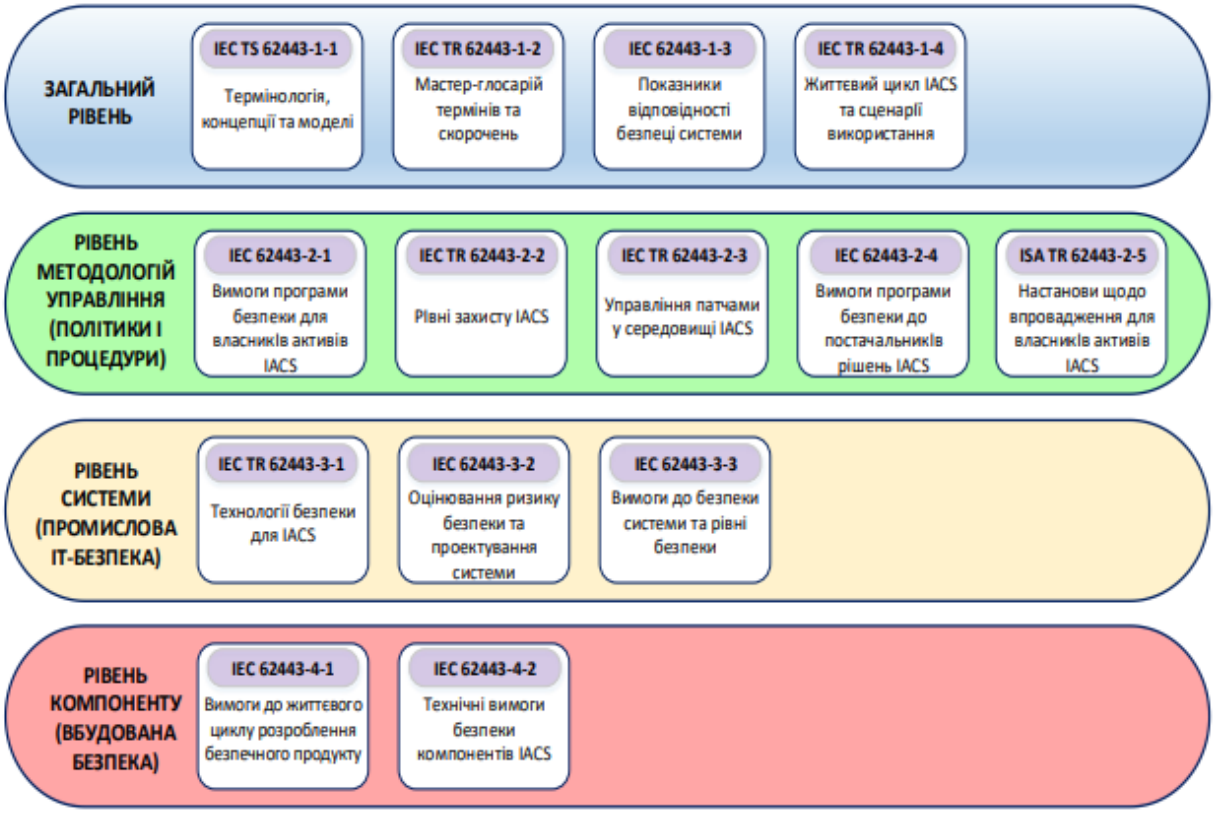

Рисунок 2.1 - Структура серії стандартів IEC 62443

У таблиці 2.1 наведено назви всіх відповідних нормативних актів серії 62443. Різні типи документів (що видаються та розробляються) виділені різними кольорами.

Таблиця 2.1 – Нормативні документи серії IEC 62443

Частина	Статус	Назва ENG/UA
IEC TS 62443-1-1-2009	Технічна специфікація	Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models *Промислові комунікаційні мережі – Інформаційна безпека мереж та систем – Частина 1-1: Термінологія, концепції та моделі*
IEC TR 62443-1-2 *	Технічний звіт	Security for industrial automation and control systems security – Part 1-1: Master Glossary of terms ans abbreviations *Безпека для систем промислової автоматизації та керування – Частина 1-1: Мастер-глосарій термінів та скорочень*
IEC TS 62443-1-3 *	Міжнародний стандарт	Security for industrial automation and control systems – Part 1-3: Cyber security system compliance metrics *Безпека для систем промислової автоматизації та керування – Частина 1-3: Показники відповідності безпеці системи*
IEC TR 62443-1-4 *	Технічний звіт	Security for industrial automation and control systems – Part 1-4: IACS security life cycle and use case *Безпека для систем промислової автоматизації та керування – Частина 1-4: Життєвий цикл системи промислової автоматизації та керування та сценарії використання*
IEC 62443-2-1-2010	Міжнародний стандарт	Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program *Промислові комунікаційні мережі - Інформаційна безпека мережі та системи – Частина 2-1: Створення програми інформаційної безпеки системи промислової автоматизації*
IEC TR 62443-2-2 *	Технічний звіт	Security for industrial automation and control systems – Part 2-2: IACS protection levels *Безпека для систем промислової автоматизації та керування – Частина 2-2: Рівні захисту системи промислової автоматизації та керування*
IEC TR 62443-2-3-2015	Технічний звіт	Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment *Безпека для систем промислової автоматизації та керування – Частина 2-3: Управління патчами в оточенні системи промислової автоматизації*
IEC 62443-2-4-2015	Міжнародний стандарт	Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers *Безпека для систем промислової автоматизації та керування – Частина 2-4: Вимоги програми безпеки до постачальників послуг з систем промислової автоматизації*
IEC TR 62443-2-5 *	Технічний звіт	Security for industrial automation and control systems – Part 2-5: Implementation guidance for IACS asset owners *Безпека для систем промислової автоматизації та керування – Частина 2-5: Настанови щодо впровадження для власників активів систем промислової автоматизації та керування*

IEC TR 62443-3-1-2009	Технічний звіт	Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems *Промислові комунікаційні мережі - Інформаційна безпека мережі та системи – Частина 3-1: Технології безпеки для систем промислової автоматизації*
IEC 62443-3-2 *	Міжнародний стандарт	Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design *Безпека для систем промислової автоматизації та керування – Частина 3-2: Оцінювання ризику безпеки та проектування системи*
IEC 62443-3-3-2013	Міжнародний стандарт	Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels *Промислові комунікаційні мережі – Інформаційна безпека мережі та системи – Частина 3-3: Вимоги до безпеки системи та рівні безпеки*
IEC 62443-4-1-2018	Міжнародний стандарт	Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements *Безпека для систем промислової автоматизації та керування – Частина 4-1: Вимоги до життєвого циклу розробки безпечного продукту*
IEC 62443-4-2-2019	Міжнародний стандарт	Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components *Безпека для систем промислової автоматизації та керування – Частина 4-2: Технічні вимоги до безпеки компонентів систем промислової автоматизації та керування*

** ще не опублікований документ*

• Стандарт 62443-1-1 вводить загальні поняття та моделі серії.

o Технічний звіт 62443-1-2 містить перелік термінів та скорочень, що використовуються у всій серії.

o Стандарт 62443-1-3 описує ряд показників, отриманих з базових вимог (FR) та системних вимог SR.

• Система управління (політика та процедури IACS): Опишіть необхідні політики та процедури для впровадження системи управління кібербезпекою.

o Стандарт 62443-2-1 описує умови, необхідні для визначення та впровадження ефективної системи управління безпекою мережі IACS. Цей стандарт відповідає серії ISO 27000.

o Стандарт 62443-2-2 містить конкретні вказівки щодо вимог до ефективної системи управління безпекою мережі IACS.

o Технічний звіт 62443-2-3 містить вказівки щодо тем управління виправленнями IACS.

o Стандарт 62443-2-4 визначає вимоги до постачальників IACS.

• Промислова IT-безпека (Системні вимоги IACS) описує вимоги до мережевої безпеки системи в середовищі IACS.

o Технічний звіт 62443-3-1 описує застосування різних технологій функціональної безпеки в середовищі IACS.

o Стандарт 62443-3-2 включає оцінку ризику та розробку системи IACS.

o Стандарт 62443-3-3 описує основи вимог безпеки та рівні забезпечення безпеки (SL).

• Вбудована безпека (вимоги до компонентів IACS): опишіть вимоги до мережевої безпеки компонентів у середовищі IACS.

o Стандарт 62443-4-1 описує вимоги до розробки продукції.

o Стандарт 62443-4-2 містить вимоги, що дозволяють детально відобразити системні вимоги (CP) підсистем та системних компонентів, які підпадають під заданий обсяг.

Вивести вимоги до кібербезпеки з вищезазначених стандартів для конкретних випадків автоматизації на підприємстві непросто. Так само вихідною точкою систем промислової автоматизації та управління повинна бути безперервність функціональної безпеки та заходів безпеки мережі. Якщо задовольняються необхідні вимоги щодо функціональної безпеки та безперервності бізнесу, середовище встановлення, випадки використання та ситуація загроз можуть бути використані як основа для розуміння загроз безпеці мережі для аналізу вимог безпеки мережі.

2.3 Основні поняття та ключові терміни

Захист в глибину - це шаровий механізм безпеки, який може збільшити безпеку всієї системи. Перевага цього механізму полягає в тому, що під час атаки, якщо впливає один рівень, інші рівні все одно можуть допомогти в обороні,

виявленні та реагуванні на атаку. Рівні (див. рис. 2.2) можна описати наступним чином:

• Рівень даних - це внутрішній шар. Він може використовуватися для списків контролю доступу та шифрування даних.

• Рівень програми - це наступний рівень для встановлення антивірусного програмного забезпечення та розширення програм.

• Рівень хоста - це наступний рівень після рівня програми, який використовується для виправлення виявлених вразливостей та автентифікації користувачів.

• Внутрішній мережевий рівень - це наступний рівень, IPsec (Інтернет-протокол безпеки) та система виявлення вторгнень (IDS), що використовується для IP-зв'язку, автентифікації та шифрування пакетів даних, що беруть участь у системі зв'язку, який виявляє вторгнення кожного користувача (авторизований або несанкціонований).

• Шар по периметру - це наступний шар, який використовується для реалізації ізоляції брандмауера та VPN.

• Фізичний рівень - це наступний рівень після периферійного, де використовуються комутатори, блокування, порти, фізичний доступ тощо.

• Рівень політики та процедур - це самий зовнішній і найновіший рівень, який визначає політику та процедури безпеки для мережі IACS.

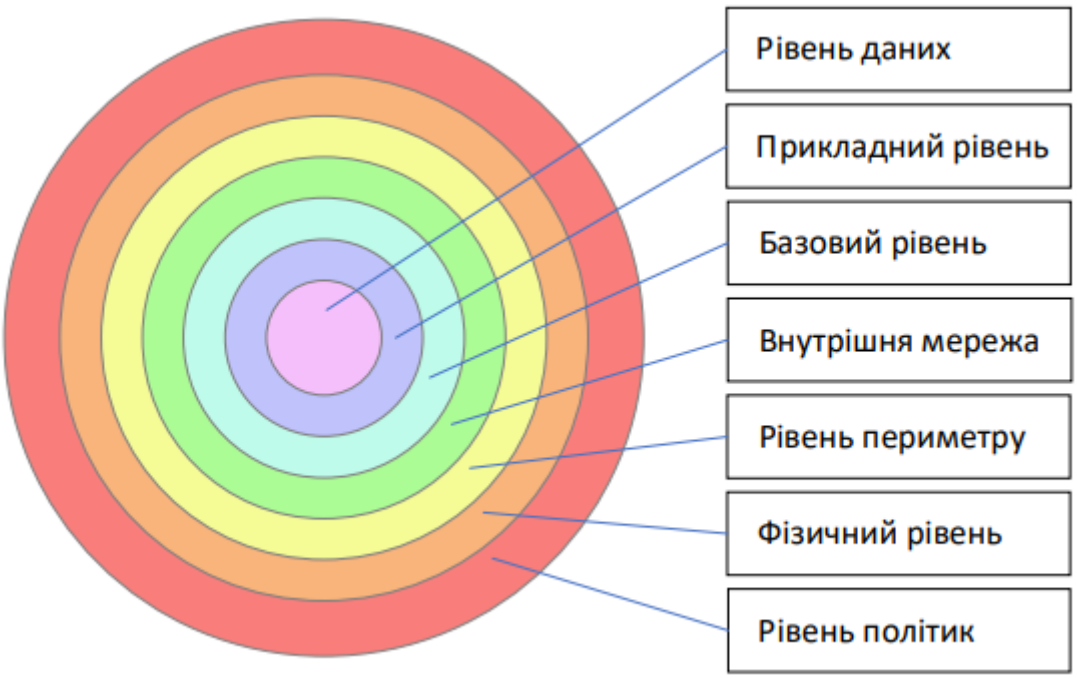

Рисунок 2.2 – Рівні захисту в глибину

Зони безпеки - це групи фізичних або логічних активів, що мають загальні вимоги до безпеки та окремі ключові компоненти системи управління.

Особливим типом зони безпеки є демілітаризована зона (DMZ), яка використовує компоненти безпеки, такі як брандмауери, для сегментації зовнішньої мережі від внутрішньої мережі IACS. Ця концепція забезпечує багатошаровий підхід до безпеки з урахуванням підходу "захист у глибині".

Умовою є особливий тип зони безпеки, який групує дані, які можна логічно об'єднати в групи потоків інформації всередині та поза зоною. Шлях може бути однією службою (наприклад, Ethernet) або декількома носіями даних. Цей шлях контролює доступ до зони, протистоячи різним атакам, таким як відмова в обслуговуванні та атаки шкідливих програм, а також захищає цілісність та конфіденційність мережевого трафіку.

На рис. 2.3 показано організацію (підприємство), яка має три заводи з незалежним корпоративним штаб-квартирою.

Три заводи A, B і C підключені до основної корпоративної мережі для забезпечення зв'язку зі штаб-квартирою та іншими заводами.

На малюнку визначено наступні чотири можливі шляхи (інші шляхи також слід визначити, але вони коротко пропущені):

• Перший - шлях усього підприємства, показаний у верхній частині графіку (позначений червоним). Він з'єднує кілька заводів у різних місцях з корпоративним центром обробки даних.

• Якщо глобальна мережа компанії будується з використанням орендованих або виділених комунікацій, це можна вважати надійним шляхом. Якщо він використовує як загальнодоступні, так і приватні мережі, його слід класифікувати як ненадійний. Все комунікаційне обладнання та брандмауери, що складають заводську систему зв'язку, включені у відповідні шляхи заводів A, B та C (позначені фіолетовим кольором).

• Три другорядні невеликі шматочки знаходяться в кожній рослині, як показано на малюнку. Кожна фабрика має свій надійний шлях, який дозволяє контролювати з’єднання.

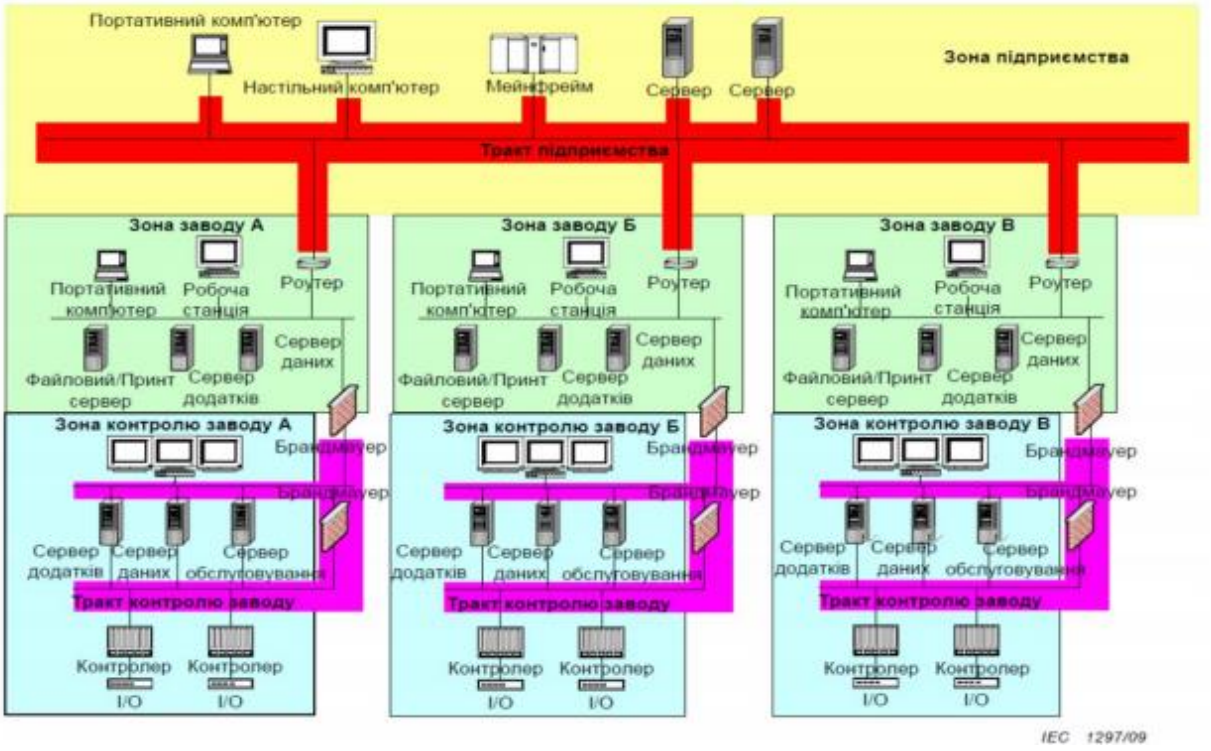

Рисунок 2.3 - Приклад тракту підприємства

2.4 Життєвий цикл кібербезпеки

Життєвий цикл кібербезпеки систем промислової автоматизації та управління з використанням циклу PDCA Шухарта-Демінга (планування, виконання, перевірка та дія) - це метод заходів безпеки, який відповідає стандартам серії ISO 27000. Стандарт визначає, а саме: розробників продуктів, системних інтеграторів та власників активів.

На рис 2.4 показаний цикл PDCA, який може бути впроваджений в промислових системах автоматизації та управління з посиланням на IEC 62443. Кожна з трьох ролей, визначених стандартом (тобто постачальник продукції, системний інтегратор та власник активів), повинна відповідати циклу PDCA.

Рисунок 2.4 – Цикл PDCA для IEC 62443

Цикл PDCA - це життєвий цикл товару для постачальників продукції, оскільки він є специфічним для продуктів чи обладнання, а для інтеграторів та власників активів - це фабричний (виробничий) життєвий цикл, оскільки він зосереджений на всій фабриці. На рис 2.5 показано життєвий цикл та процес взаємодії продуктів та фабрик у формі розробки продукту постачальника чи виробника, інтеграції або

налагодження системного інтегратора та експлуатації та обслуговування власника активу. Цей безперервний процес циклічно виконується PDCA.

Рисунок 2.5 – Життєвий цикл продуктів та виробництва з прив’язкою до безпеки

2.5 Рівні безпеки на основі IEC 62443 3-3 та IEC 624434-2

Концепція рівня безпеки SL фокусується на галузі систем промислової автоматизації IACS. Вважається, що рівень безпеки запозичений із запропонованих раніше функціональних рівнів безпеки, які успішно використовуються в промислових системах автоматизації та управління, а саме рівня цілісності безпеки (SIL).

Рівень безпеки SL забезпечує вказівки щодо прийняття рішень щодо використання контрзаходів та обладнання з різними властивими функціями безпеки. Концепція може бути використана для вибору обладнання промислової автоматизації IACS та контрзаходів, які будуть використовуватися в даній місцевості, і надає можливість класифікувати ризики конкретної зони або каналу.

Рівень безпеки SL також може бути використаний для визначення ієрархічної стратегії глибокого захисту зони, включаючи технічні заходи, засновані на апаратному та програмному забезпеченні. Рівень безпеки, визначений для компонентів, базується на чотирьох типах категорій пристроїв, визначених стандартом, а саме на вбудованих пристроях, хост-пристроях, мережевих пристроях та прикладному програмному забезпеченні.

Рівень безпеки в стандарті визначається наступним чином:

• SL 1 - Запобігання несанкціонованому розголошенню інформації шляхом підслуховування або випадкового опромінення;

• SL 2 - Використовуйте прості методи з низькими ресурсами, загальними навичками та низькою мотивацією для запобігання несанкціонованому розголошенню інформації суб’єктам, які активно шукають інформацію;

• SL 3 - Використовуйте складні інструменти з помірними ресурсами, специфічними навичками IACS та помірною мотивацією для запобігання несанкціонованому розголошенню інформації суб’єктам, які активно шукають інформацію;

• SL 4 - Використовуйте складні інструменти з розширеними ресурсами, специфічними навичками IACS та високою мотивацією для запобігання несанкціонованому розголошенню інформації суб’єктам, які активно шукають інформацію.

У таблиці 2.2 подано короткий опис рівнів безпеки, а також додаткову інформацію про рівень хакерів та використовувані інструменти.

Таблиця 2.2 – Рівні безпеки SL

Рівень безпеки	Опис	Ціль	Навички	Мотивація	Застосування засобів
SL 1	Можливість захисту від причинного або випадкового порушення	Неправильне налаштування	Немає обізнаності	Несистематична	Розрізнено
SL 2	Можливість захисту від навмисних порушень за допомогою простих засобів з низькими ресурсами, загальними навичками та низькою мотивацією	Не вжито заходів безпеки, атакуючий - хакер	Базові	Низька	Цілеспрямовано
SL 3	Можливість захисту від навмисних порушень за допомогою складних засобів із помірними ресурсами, специфічними навичками IACS та помірною мотивацією	Виконуються лише помірні заходи безпеки, хакінг високого рівня	Притаманні промисловому домену	Середня	Навмисно
SL 4	Можливість захисту від навмисних порушень за допомогою складних засобів із розширеними ресурсами, специфічними навичками IACS та високою мотивацією	Економічний збуток	Специфічні промислові	Висока	Агресивно

2.6 Рівні зрілості на основі IEC 62443 2-4 та IEC 62443 4-1

Рівень зрілості базується на інтеграції моделі можливостей зрілості послуги (CMMI-SVC). Ці рівні визначають базовий рівень, який повинен відповідати вимогам, зазначеним у IEC 62443 2-4 та IEC 62443 4-1. Порівняно з попереднім рівнем, кожен рівень буде поступово вдосконалюватися. Постачальникам послуг та власникам активів потрібно визначити рівень зрілості, пов'язаний із виконанням кожної вимоги.

У таблиці 4 узагальнено кожен рівень зрілості (ML), а також класифікація та опис кожного рівня.

Таблиця 2.3 – Рівні безпеки

Рівень зрілості	Категорія	Опис
ML 1	Начальний	Здатність надати послугу без підтримки документально підтвердженого процесу, який погано контролюється
ML 2	Керований	Здатність надати послугу за підтримкою формально документованого процесу із доказом досвіду та підготовленим персоналом
ML 3	Визначений	Здатність відповідати рівню зрілості ML2, включаючи доказ тренування персоналу, наприклад задокументований процес плюс учасники процесу підготовки кадрів
ML 4	Вдосконалений	Здатність відповідати рівню зрілості ML2, включаючи демонстрацію постійного вдосконалення, наприклад звіт про внутрішній аудит

Цільова аудиторія серії стандартів ISA 99 / IEC62443

Цільова аудиторія стандарту ISA99 / IEC 62443:

-Постачальники продуктів (розробники продуктів) для небезпечних виробництв.

-Системний інтегратор.

-Власник активу.

Ці ролі складають основу для ідентифікації та з'єднання різних частин серії IEC 62443, як показано на рисунку 6 нижче.

Рисунок 2.6 – Розподілення ролей у серії 62443

Рисунок 2.6 ілюструє, як продукція, розроблена постачальником продукції, пов'язана з обслуговуванням та інтеграцією системного інтегратора та роботою власника активу. Тут також пояснюються ролі та взаємозв'язки між постачальниками продукції, системними інтеграторами та власниками активів.

• Постачальники продуктів несуть відповідальність за розробку та тестування систем управління, включаючи програми (антивірус, білий список тощо), вбудовані пристрої (програмовані логічні контролери PLC, розподілені системи управління DCS тощо), мережеве обладнання (брандмауери, маршрутизатори, комутатори тощо). .) Тощо), як хост-пристрій (станція оператора, інженерна станція тощо), що співпрацює із системою або підсистемою, визначеною в IEC 62443-3-3, IEC 62443-4-1, IEC 62443-4-2.

• Системні інтегратори відповідають за інтеграцію та впровадження продуктів у рішення для автоматизації з використанням процесів, сумісних з IEC 62443-2-4, IEC 62443-3-2, IEC 62443-3-3.

• Власник активу відповідає за експлуатаційну спроможність та підтримку політики та процедур впровадження систем автоматизації польової автоматизації, зазначених у IEC 62443-2-1, IEC 62443-2-3 та IEC 62443-2-4.

Життєвий цикл кібербезпеки

ISA / IEC 62443 визначає життєвий цикл мережевої безпеки як міцну основу для захисту систем промислової автоматизації. Життєвий цикл мережевої безпеки - це процес, що складається з чотирьох основних етапів, як показано на рисунку 2.7.

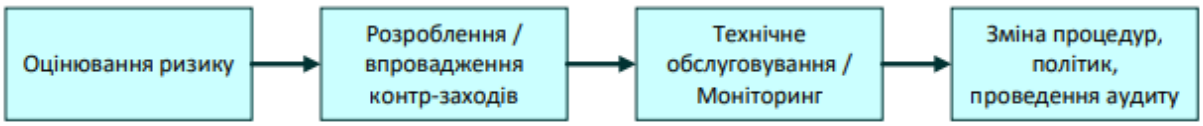

Рисунок 2.7 – Життєний цикл кібербезпеки

Оцінка фазового аналізу систем промислової автоматизації та управління. Розподіліть активи за зонами та встановіть шляхи зв’язку між ними. На цьому етапі потрібно виявити вразливі місця, розрахувати ризики та визначити пріоритети на основі відносних ризиків.

Кібербезпека промислових систем

Фаза впровадження - Вклад на цю фазу є результатом оцінки та визначення пріоритетів ризиків та вразливостей на етапі оцінки, якщо він використовується для створення детальних вимог безпеки. У свою чергу, ці вимоги використовуються для формулювання та реалізації контрзаходів, які можуть бути представлені у вигляді застосованої технології, політики компанії або організаційної практики (навчання, підзвітність тощо).

Етап технічного обслуговування - На цьому етапі компанія активно контролює системи промислової автоматизації, реагує на інциденти, виконує завдання технічного обслуговування (резервне копіювання, ремонт тощо) та керує змінами.

Фаза постійного вдосконалення - це фаза аналізу уроків, отриманих в результаті інциденту, впровадження необхідних змін та регулярного аудиту. У цьому розділі основна увага приділяється останнім двом етапам: технічному обслуговуванню та постійному вдосконаленню, оскільки вони мають важливе значення для постійної безпеки промислових систем управління.

Фаза технічного обслуговування включає різні незалежні заходи, які вимагають постійного та ефективного управління. Події можна розділити на два ключові типи: події, що відбуваються безперервно, та події, що відбуваються після події. Кожен з них буде детально обговорений.

Компанія здійснює дві основні види діяльності з використанням систем промислової автоматизації та управління - моніторинг активів та контроль безпеки:

• Постійний моніторинг системи. Мережа, що використовується для відстеження пристроїв, підключених до систем, що використовують найновіше програмне забезпечення. Будь-які нові пристрої, додані до системи, повинні бути ретельно досліджені. Моніторинг активів, як правило, забезпечується внутрішніми або сторонніми інструментами та програмами;

• Постійний моніторинг безпеки. На етапі реалізації життєвого циклу мережевої безпеки можуть бути додані різні засоби та системи безпеки, включаючи системи виявлення вторгнень у мережу, програмне забезпечення інформації про безпеку та управління подіями (SIEM), антивірусні програми та інші системи безпеки. Ця поточна діяльність зосереджена на точному відстеженні технологій, які були впроваджені для виявлення шкідливої діяльності. Звіти про несприятливі події, отримані від цих систем, повинні оцінюватися та оброблятися персоналом у процесі обробки подій (англ. incident handling).

Моніторинг безпеки мережі не такий простий, як перевірка повідомлень після того, як працівники щоранку виходять на роботу. Персонал повинен повністю розуміти програми, що використовуються для моніторингу та спотворення систем

безпеки, і вміти налаштовувати інструменти та системи, що використовуються для контролю безпеки, для оптимізації їх точності.

Заходи мережевої безпеки під час технічного обслуговування

На додаток до діяльності, яка продовжує виконуватися у фоновому режимі, багатьма компонентами фази технічного обслуговування також управляють за допомогою подій.

Управління патчами. Постачальники обладнання використовують виправлення для усунення вразливостей, тому вони є критично важливими для мережевої безпеки системи. Виправлення можна застосовувати до систем захисту кінцевих точок та систем виявлення вторгнень для оновлення підписів шкідливих програм. Традиційно компанії з системами промислової автоматизації оновлюють своє програмне забезпечення під час запланованих відключень системи. Однак цей метод не сумісний з вимогами безпеки мережі. Системи промислової автоматизації та управління повинні мати можливість розподіляти встановлення виправлень безпеки між запланованими відключеннями.

Перш ніж встановлювати в систему, необхідно оцінити потенційні виправлення. Цей патч може усунути уразливість, яка не є проблемою для системи промислової автоматизації, і в цьому випадку її не слід встановлювати. Наприклад, виправлення вразливості протоколу передачі файлів (FTP) не є проблемою для пристроїв, які вимкнули FTP. Слід проаналізувати нові виправлення, щоб визначити, чи є нові вразливості, які збільшують ризик, ніж усунені вразливості. Пластирі також повинні бути протестовані в пісочниці перед тим, як розміщувати їх у виробничій мережі.

Якщо компанія, яка є власником пристрою IACS, веде список усіх пристроїв / програм, процес управління виправленнями можна спростити. Вам потрібно визначити процес, який вимагає від працівників періодичного перегляду програмного забезпечення для виправлення виявлених уразливостей.

Програмні виправлення для апаратного забезпечення зазвичай завантажуються з підприємства на сервер виправлень, який знаходиться в демілітаризованій зоні між підприємством та мережею управління.

Резервне копіювання системи. Компанії, що володіють IACS, зазвичай мають внутрішні рекомендації або політики, що визначають процес резервного копіювання системи. Такі стратегії визначають елементи для резервного копіювання, інтервал резервного копіювання, кількість резервних копій, ручні або автоматичні резервні копії, плани резервного копіювання, місця зберігання файлів (повинно бути в безпечному місці) та вказують, як правильно керувати системою резервного копіювання. термін служби досягнутий. Стратегія резервного копіювання може також вимагати певних функцій, таких як підпис коду, для забезпечення цілісності резервних копій файлів. Слід зазначити, що якщо компанія стикається з інцидентом безпеки, їй слід регулярно перевіряти резервне копіювання файлів та відновлення функцій, щоб забезпечити нормальну роботу системи.

Управління змінами. На етапі реалізації були створені схеми, що описують архітектуру системи, мережу, перелік активів та різні додаткові документи. Зміни відбуваються під час роботи системи - коли замінюються нові модулі, підсистеми, зміни мережі або обладнання. Кожна зміна може вимагати не лише фіксованого системного документа, а й відповідних змін у самому документі. Для забезпечення ефективного прийняття рішень, впровадження та документування у компаніях із системами промислової автоматизації та контролю слід запровадити офіційні процеси управління змінами. В іншому випадку документація буде недостовірною, що може спричинити неполадки.

Обробка подій. Одним з найбільш критичних процесів на етапі технічного обслуговування є реагування на аварії та обробка. Обробник інцидентів розробив план боротьби з несанкціонованими вторгненнями, крадіжками мережі, відмовою в обслуговуванні, шкідливим кодом та іншими інцидентами безпеки мережі. Ключовим результатом є створення та розповсюдження плану реагування на аварії.

2.6 Висновки до розділу 2

Стандарти серії IEC 62443 мають сучасний підхід до кібербезпеки. Задають вимоги до проектування накладених систем управління кібербезпекою АСУ ТП і

SCADA і до проектування АСУ ТП з уже закладеними і інтегрованими заходами безпеки. Метою серії IEC 62443 є підвищення функціональної безпеки, доступності, цілісності та конфіденційності компонентів або систем, що використовуються в промисловій автоматизації, включаючи аспекти закупівель. Основні відмінності від ISO/IEC 27000 :

• Деякі інші аспекти функціональної безпеки, здоров'я та навколишнього середовища, які не пропонуються в ISO / IEC 27001 та ISO / IEC 27005);

• Існування деяких додаткових термінів та визначень.

3 ДОСЛІДЖЕННЯ ПРОБЛЕМ ВПРОВАДЖЕННЯ ТА СЕРТИФІКАЦІЇ СУІБ НА ОСНОВІ IEC 62443

3.1НААУ

Національне агентство з акредитації України (НААУ) є національним агентством з акредитації України.

Основними функціями агентства є:

• Акредитація органом з оцінки відповідності (ООВ);

• Контролювати відповідність акредитаційних вимог органами з акредитації.

Агентство регулюється українським законодавством, міжнародними стандартами ISO / IEC17011 та документами міжнародних сертифікаційних організацій (EA, IAF, ILAC).

Одним із пріоритетів українського уряду є приведення системи регулювання технологій в Україні у відповідність до вимог Світової організації торгівлі та Європейського Союзу. Виконання цього завдання є надзвичайно важливим для України, оскільки Україна стала членом Світової організації торгівлі 16 травня 2008 року, а переговори з державами-членами ЄС щодо створення зони вільної торгівлі тривають.

Ключовим фактором реформування системи нагляду за технологіями є приведення системи акредитації України у відповідність до вимог Європейської асоціації акредитації та підписання угоди про акредитацію між Українським національним агентством з акредитації та Європейською асоціацією акредитації. Історія створення У 2001 році Україна прийняла Закон про акредитацію органів з оцінки відповідності, який встановлює правові, організаційні та економічні принципи акредитації органів з оцінки відповідності в Україні. Відповідно до закону, Міністерство економіки створило Українське національне агентство з сертифікації у 2002 році. Крім того, створено комітет з сертифікації, комітет з технічної сертифікації та апеляційний комітет.

Сфера діяльності

NAAU сертифікує органи з оцінки відповідності (ООВ) у наступних областях:

• Органи з сертифікації персоналу - відповідають вимогам ISO / IEC 17024: 2003 (перехід на нову версію стандарту ISO / IEC17024: 2012) "Загальні вимоги до органів з сертифікації персоналу";

• Випробувальні та калібрувальні лабораторії - відповідно до ДСТУ ISO / IEC 17025: 2006 "Загальні вимоги до компетентності випробувальних та калібрувальних лабораторій");

• Орган із сертифікації системи управління - відповідає вимогам ISO / IEC 17021: 2011 "Вимоги до організацій, які здійснюють аудит та сертифікацію систем управління";

• Інспекційне агентство - відповідно до вимог ДСТУ ISO / IEC 17020-2001 (перехід до нової версії стандарту ISO / IEC 17020: 2012) щодо "оцінки відповідності". «Вимоги до діяльності різних типів інспекційних установ» (отримано у 2014 році);

органи з сертифікації продукції — згідно з вимогами ISO/IEC 17065 «Оцінювання відповідності — Вимоги до органів, що сертифікують продукцію, процеси та послуги».

Співробітництво з Європейською кооперацією з акредитації (ЕА)

Основним європейським механізмом діяльності НААУ є співпраця з Європейською організацією сертифікаційного співробітництва (ЄА), яка керує системою експертної оцінки відповідно до Регламенту (ЄС) № 765/2008, оприлюдненого 9 липня 2008 року. Національні органи з акредитації держав-членів ЄС та інших європейських країн. ЕА має багатосторонню угоду (EA MLA) та двосторонню угоду (EA BLA), і її підписанти, національні органи з сертифікації, визнають, що їх системи сертифікації рівнозначні.

У 2004 році НААУ підписало угоду про співпрацю з ЕА.

У 2009 році, після двох оцінок (2006 та 2009), НААУ було акредитовано у галузі "Акредитація органів з сертифікації персоналу".

2011-НААУ отримав статус асоційованого члена ЕА.

2012-NAAU розширив акредитацію ЕА у галузі калібрування та сертифікації випробувальних лабораторій згідно з ISO / IEC 17025: 2006 "Загальні вимоги до

компетенції випробувальних та калібрувальних лабораторій" та органу з сертифікації системи управління відповідно до ISO / IEC 17021: 2011 "організації" Вимоги до систем управління аудитом та сертифікацією ".

У жовтні 2014 року на засіданні Ради багатосторонньої угоди ЕА (ЕА IAS), яке відбулося в Брюсселі (Королівство Бельгія) з 1 по 2 жовтня 2014 року, було вирішено розширити визнання НААУ у цій галузі відповідно до ISO / IEC 17020. інспекційне агентство проводить сертифікацію.

У жовтні 2015 року під час засідання ЕА IAS, що відбулося в Берліні (Німеччина), було прийнято рішення про розширення акредитації NAAU у галузі акредитації органу з сертифікації продукції.

У жовтні 2015 року Комітет багатосторонньої угоди ЕА вирішив надати продовження двосторонньої угоди НААУ про сертифікацію "Сертифікація продукції".

26 листопада 2015 року НААУ підписало угоду про акредитацію ЕА у галузі "органів із сертифікації продукції", що створило умови для підписання Україною угоди АСАА (стаття 57 Угоди між Україною та ЄС: Угода про оцінку відповідності та прийняття промислової продукції) .

Співпраця з Міжнародною асоціацією акредитації лабораторій (ILAC)

У 2004 році НААУ отримало статус афілійованого члена ILAC.

У 2013 році, згідно з пунктом 30 "Забезпечити підписання НААУ та Міжнародною організацією співробітництва з питань акредитації лабораторій ILAC угоди про акредитацію", впровадити план дій.

У відповідь на стратегію розвитку системи регулювання технологій до 2018 року керівництво NAAU вирішило ще більше поглибити співпрацю між NAAU та ILAC, особливо приєднавшись до NAAU для приєднання до Угоди про взаємне визнання ILAC (ILAC MRA).

16 вересня 2014 року НААУ отримало статус асоційованого члена ILAC.

24 вересня 2014 р. НААУ отримав статус повноправного члена ILAC та став підписантом угоди ILAC MRA у галузі калібрування та випробувань відповідно до

міжнародного стандарту ISO / IEC 17025 «Загальні вимоги до випробувань та можливостей випробувань.

11 грудня 2014 року НААУ розширило сферу акредитації відповідно до міжнародного стандарту ISO / IEC 17020 "Загальні стандарти діяльності різних інспекційних установ" та стало підписантом угоди ILAC MRA у галузі інспекції.

Структура національної системи акредитаціїї

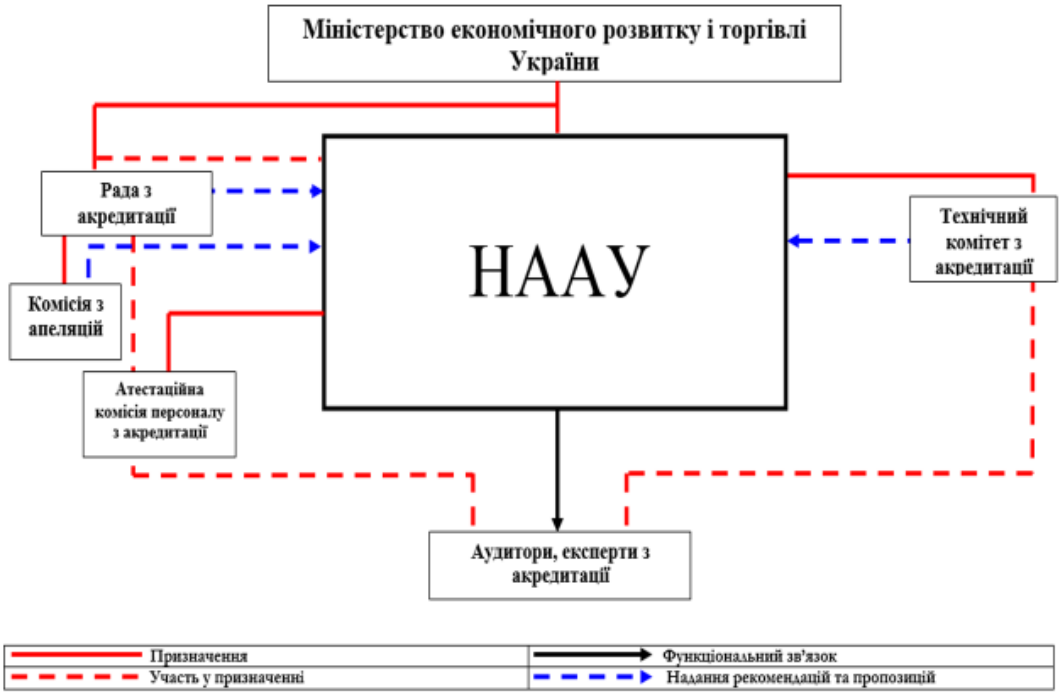

Рисунок 3.1 – Структура НААУ

Кілька глобальних органів з сертифікації також створили програми сертифікації IEC 62443. Ці плани базуються на посиланнях на стандарти та процедури, що описують їх методи тестування, політику наглядового аудиту, політику публічних документів та інші конкретні аспекти їх планів. Програма сертифікації кібербезпеки IEC 62443 забезпечується багатьма визнаними центральними банками по всьому світу, включаючи exida, CertX, SGS-TÜV Saar, TÜV Nord, TÜV Rheinland, TÜV SÜD та UL. Безстороння сторонння організація, яка

називається органом із сертифікації (СВ), акредитована для роботи відповідно до ISO / IEC 17065 та ISO / IEC 17025. Орган з сертифікації акредитований для прийняття аудиту, оцінки та тестування органу з акредитації (АВ).У кожній країні часто існує один національний АБ. Ці АБ діють відповідно до вимог ISO / IEC 17011, стандарту, який містить вимоги до компетентності, послідовності та неупередженості органів з акредитації при акредитації органів з оцінки відповідності. АБ є членами Міжнародного форуму з акредитації (IAF) для роботи в системах управління, продуктів, послуг та акредитації персоналу або Міжнародного співробітництва з акредитації лабораторій (ILAC) для акредитації лабораторій. Багатостороння угода про визнання (ПДП) між АБ забезпечить загальне визнання акредитованих ЦБ.

Стандарт кібербезпеки IEC-62443 - це багатогалузевий стандарт, у якому перелічені методи та технології кібербезпеки. Ці документи є результатом процесу розробки стандарту IEC, в якому пропозиція ANSI / ISA-62443 та інші матеріали подаються до комітету країни, що розглядається, та коментуються зміни. Коментарі розглядаються різними комітетами IEC 62443, де вони обговорюються та вносяться зміни за погодженням. Багато членів комітету IEC є членами комітету ISA S99. Сьогодні використовуються основні концепції оригінального документа ANSI / ISA 62443.

Щодо серії міжнародних стандартів ISO / IEC 27001, слід зазначити, що, як національний стандарт України, лише перша версія ISO / IEC 27001 визнана та використовується у банківській галузі у формі вимоги до СОУ Н НБУ 65.1 SUIB 1.0: 201010 (Відповідно до закону "Основні принципи, що стосуються кібербезпеки України" Національний банк України є одним із суб'єктів національної системи кібербезпеки. На жаль, в інших галузях промисловості ці стандарти не використовуються з різних причин, головним чином через відсутність законів і норм. Хоча міжнародні стандарти інформаційної безпеки ISA 099 та IEC 62443 є відкритими стандартами, спеціально застосовними до приватної критичної інфраструктури. Згідно з результатами аналізу зарубіжного досвіду, з метою запобігання недобросовісній конкуренції та монополізації регуляторної діяльності у

цій галузі сформуйте та використовуйте альтернативні стандарти та моделі мережевої безпеки, призначені для приватного сектору в різних галузях.

3.2 Реалізація серії 62443

Хоча документи IEC 62443 мають багато переваг, на жаль, як показують результати опитування (розділ 4.2), існують великі проблеми при впровадженні українських компаній.

Основними перешкодами на даний момент є:

1. Серія IEC 62443 наразі неповна. Деякі технічні характеристики ще не оголошені.

2. Зміст серії IEC 62443 є вичерпним: поточна загальна довжина перевищує 800 сторінок, і очікується, що найближчим часом буде більше специфікацій. Щоб зрозуміти всю серію, потрібно багато часу та зусиль.

3. Вартість отримання повної копії стандарту на офіційному веб-сайті Міжнародної електротехнічної комісії становить понад 2600 доларів США.

4. Стандарти та нормативні документи, як правило, швидко змінюються, тому дуже важливо регулярно їх переглядати та якомога швидше оновлювати національні стандарти. Наприклад, 2020 рік є кінцевим строком для стабілізації наступних норм 62443-1-1, 62443-2-1, 62443-2-3, 62443-2-4 та 62443-3-1. Це означає, що коли цей офіційний документ буде офіційно опублікований (кінець листопада 2019 р.), З цим документом буде пов’язаний лише один календарний місяць. Швидше за все, вони будуть діяти протягом 2020 року. Положення про стабільність базується на оцінці зрілості та майбутнього технології, а також очікуваних змін, пов'язаних з розробкою або підтримкою відповідної публікації. Зазвичай вони тривають від 3 до 12 років. Якщо комітету потрібно обробити поправки або переглянути до дати офіційного розгляду, він може визначити дату розгляду та відповідно змінити дату стабілізації. 62443-3-3-2021, 62443-4-1-2022 та 62443-4-2-2023 стабільний період.

5. В Україні бракує ринку сертифікаційних центрів, який би міг засвідчити, що продукція відповідає стандартам серії 62443.

6. Культура українських компаній, що використовують стандарти безпеки, сформувалася. На жаль, лише під впливом зовнішніх факторів відбуваються як успішні атаки на об’єкти та / або системи критичної інфраструктури, так і обов’язкові норми в нормативних актах.) регламентує процедури забезпечення безпеки, а невиконання буде суворо каратися відповідно до певних процедурних правил.

Єдина основа для кібербезпеки та функціональної безпеки

Єдина концепція безпеки та безпечне середовище

Залишається ще одна проблема: як поєднати вимоги безпеки мережі з вимогами функціональної безпеки, що дуже важливо, оскільки системи промислової автоматизації управляють потенційно небезпечними фізичними об’єктами, і це є їх основним ризиком.

Буває, що експерти з кібербезпеки не до кінця ознайомилися з деталями систем промислової автоматизації, тобто якщо система не атакується, то проблем немає. Але загрози та ризики походять не лише від злочинців, але й від некомпетентних працівників, несправності обладнання та впливу на навколишнє середовище. Ці проблеми вже були вирішені в рамках функціональної безпеки за допомогою методів забезпечення надійності та управління процесом життєвого циклу. Фахівці з функціональної безпеки справді скептично ставляться до кібербезпеки, але конкретних кіберзагроз вони не виявили. Системи безпеки дуже консервативні, оскільки вимагають високих витрат на ліцензування та сертифікацію. В даний час не існує іншого шляху, як напружена робота та інтеграція знань у різні дисципліни.

Для сучасних промислових систем важливо використовувати методи, призначені для забезпечення мережевої безпеки та функціональної безпеки. Слід зазначити, що у стандартах функціональної безпеки серії IEC 61508 не згадується мережева безпека і не вказуються методи, а посилаються на стандарти серії IEC 62443.

Багато галузевих настанов, стандартів та технічних специфікацій сформульовано в галузі мережевої безпеки та функціональної безпеки. Однак галузь

очікує зведеного документу функцій та систем безпеки мережі в значній мірі. У цих документах навіть терміни "функціональна безпека" та "мережева безпека" іноді мають різне значення. Тому важко застосовувати їх у цілому до виробничої системи одночасно.

В IEC 61508 (усі частини) основний акцент робиться на реалізованих функціях безпеки, а опис архітектури більше пов'язаний з апаратною стійкістю до відмов (HFT) та стійкістю до відмов системи. Однак для всіх зазначених систем не існує чіткої архітектури. На відміну від них, показники цілісності безпеки, такі як рівень цілісності безпеки (SIL) та здатність системи (SC), визначені в IEC 61508 (усі частини), дозволяють визначати функціональну безпеку та пов'язані з цим несправності спеціалізованих промислових систем на відносно низькому рівні Набір адекватних заходів для усунення несправностей системи.

Рисунок 3.2 узагальнює взаємозв'язок між функціями системи промислової автоматизації, включаючи роль функціональної безпеки, основних функцій, основних функцій управління та додаткових функцій.

Рисунок 3.2 - взаємозв'язок функцій систем промислової автоматизації

Основна функція також включає функціональну функцію безпеки системи промислової автоматизації. Основні функції, визначені в результаті оцінки на площині "ризик загрози" (безпека мережі), можуть бути реалізовані в спеціальній системі, що стосується безпеки (англійська система, пов'язана з безпекою), або в іншій системі, крім цієї.

Технічний звіт IEC TR 63069: 2019 "Вимірювання, управління та автоматизація промислових процесів-основи функціональної безпеки та забезпечення" ("Вимірювання, управління та автоматизація функціональних систем безпеки та забезпечення промислового процесу") вводить ідею безпечного середовища English Environment Environment) та досягли домовленості щодо напрямків співпраці між функціональним полем безпеки та кібербезпекою.

Середовище безпеки - це сукупність загальних контрзаходів, необхідних для забезпечення ефективного середовища захисту для виконання функціональних функцій безпеки, але це не обмежується захистом його функцій.

На рисунку 3.3 показано взаємозв'язок між середовищем безпеки, робочим середовищем та системами, що стосуються безпеки.

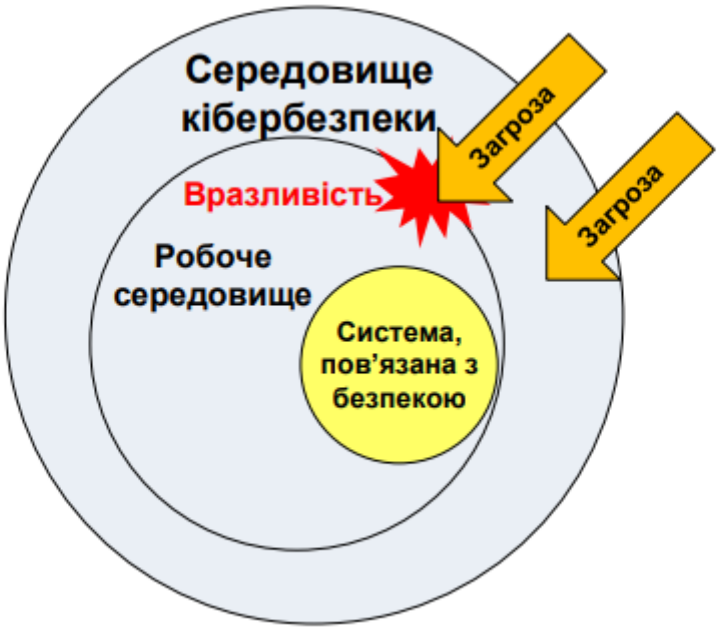

Рисунок 3.3 – Середовище безпеки

Середовище безпеки включає, але не обмежується наступними контрзаходами:

• Захистити всі контрзаходи, що оточують оцінене середовище безпеки мережі;

• усі контрзаходи щодо взаємодії між різними функціональними підрозділами в середовищі безпеки;

• Усі контрзаходи, що застосовуються до функціональних елементів у безпечному середовищі.

Примітка 1. Для практичного застосування протидії можуть бути не лише функціями безпеки.

Примітка 2: Середовище безпеки відрізняється від "зони", описаної в серії IEC 62443.

Примітка 3: Середовище безпеки може включати стратегію поглибленого захисту (див. IEC TS 62443-1-1: 2009, стаття 5.4) для досягнення достатньої гнучкості програми.

Заходи безпеки можуть бути інтегровані в будь-яку функціональну частину технічної системи, включаючи функціональні блоки систем безпеки.

Структура, описана в IEC 62443 (усі частини), включає поняття району, яке передбачає, що межі безпеки повинні бути чітко визначені для конкретної зони, а між зонами повинні бути встановлені спеціальні зв’язки, які називаються шляхами. Одна або декілька ділянок або шляхів можуть бути використані як контрзаходи для безпечного середовища.

путівник

Цей розділ додатково визначає рекомендації високого рівня, які згадуються як настанови в технічному звіті IEC TR 63069: 2019, з міркувань безпеки, пов’язаних із функціями безпеки промислової автоматизації та систем управління.

Критерій 1: Захистити реалізацію функціональних функцій безпеки.

Заходи безпеки повинні ефективно запобігати або запобігати загрозам негативного впливу на системи, пов'язані з безпекою, та функціональні функції безпеки, що реалізуються ними. Оцінка функціональних функцій безпеки повинна базуватися на припущенні ефективних заходів протидії безпеці.

ПРИКЛАД 1:

1) Очікується, що контрзаходи безпеки запобігають несанкціонованому внесенню змін у відповідне програмне забезпечення функціональної безпеки, наприклад, через віддалений доступ.

2) Дослідження безпеки та програмного забезпечення або інші заходи, пов’язані з процесами, можуть запобігти ненавмисному використанню шкідливого програмного забезпечення в коді, що має важливе значення для безпеки.

Критерій 2: Захистити реалізацію функцій безпеки.

Функціональні заходи безпеки не повинні негативно впливати на ефективність впровадження безпеки.

Примітка: Людський фактор слід враховувати з точки зору функціональної безпеки та загальної безпеки.

Приклад 2:

1) Реалізація функціональної безпеки забороняється додавати функції, які не будуть оцінюватися з точки зору безпеки (наприклад, системи віддаленого доступу).

2) Впровадження функціональної безпеки може бути більш чутливим до атак відмови в обслуговуванні, а отже, може стати потенційною метою, яка негативно впливає на доступність системи.

Критерій 3: Сумісність безпечного впровадження

Реалізація функції функціональної безпеки та реалізація функції безпеки не можуть мати несприятливого протиріччя.

Приклад 3:

1) На швидкість зв'язку системи впливають заходи безпеки, тому вони негативно впливають на часовий аспект функціональної функції безпеки.

2) Метод пароля (англійська), що використовується для забезпечення безпеки, не може негативно вплинути на захист каналу зв'язку, що використовується для реалізації функціональних функцій безпеки. Через пом'якшення ризиків функціональної безпеки та безпеки та через те, що ці системи взаємопов'язані, пріоритет не визначається.

Зв'язок та взаємодія між доменами функціональної безпеки та безпеки повинні проходити протягом усього життєвого циклу, щоб забезпечити відповідне середовище безпеки для основних функцій систем промислової автоматизації та управління, включаючи діяльність з функціональної безпеки.

Загалом рекомендуються такі заходи:

1. Розвиток функцій продукту, пов’язаних з функціональною безпекою та безпекою, повинно здійснюватися паралельно, а інформація про діяльність із впровадження функцій безпеки повинна поширюватися серед усіх ключових зацікавлених сторін;

2. Вирішення конфліктів повинно базуватися на консенсусі, досягнутим зацікавленими сторонами обох сторін;

3. До монтажу та введення в експлуатацію зацікавлені сторони у двох сферах повинні забезпечити сумісність заходів протидії безпеці з експлуатацією та технічним обслуговуванням систем, що стосуються безпеки.

Функціональна безпека означає нормальну роботу систем, що стосуються безпеки. Для систем, де функціональна безпека залежить від систем, пов’язаних з безпекою, протидії безпеці допомагають виконувати функції функціональної безпеки. Комплекс контрзаходів щодо безпеки повинен створити безпечне середовище для досягнення цієї мети.

Рекомендується, щоб експерти з функцій та захисту інформації взаємодіяли між собою для забезпечення загальної безпеки. Конкретна реалізація взаємодії залежить від політики організації. Огляд потенційних взаємодій наведено на рисунку 3.4.

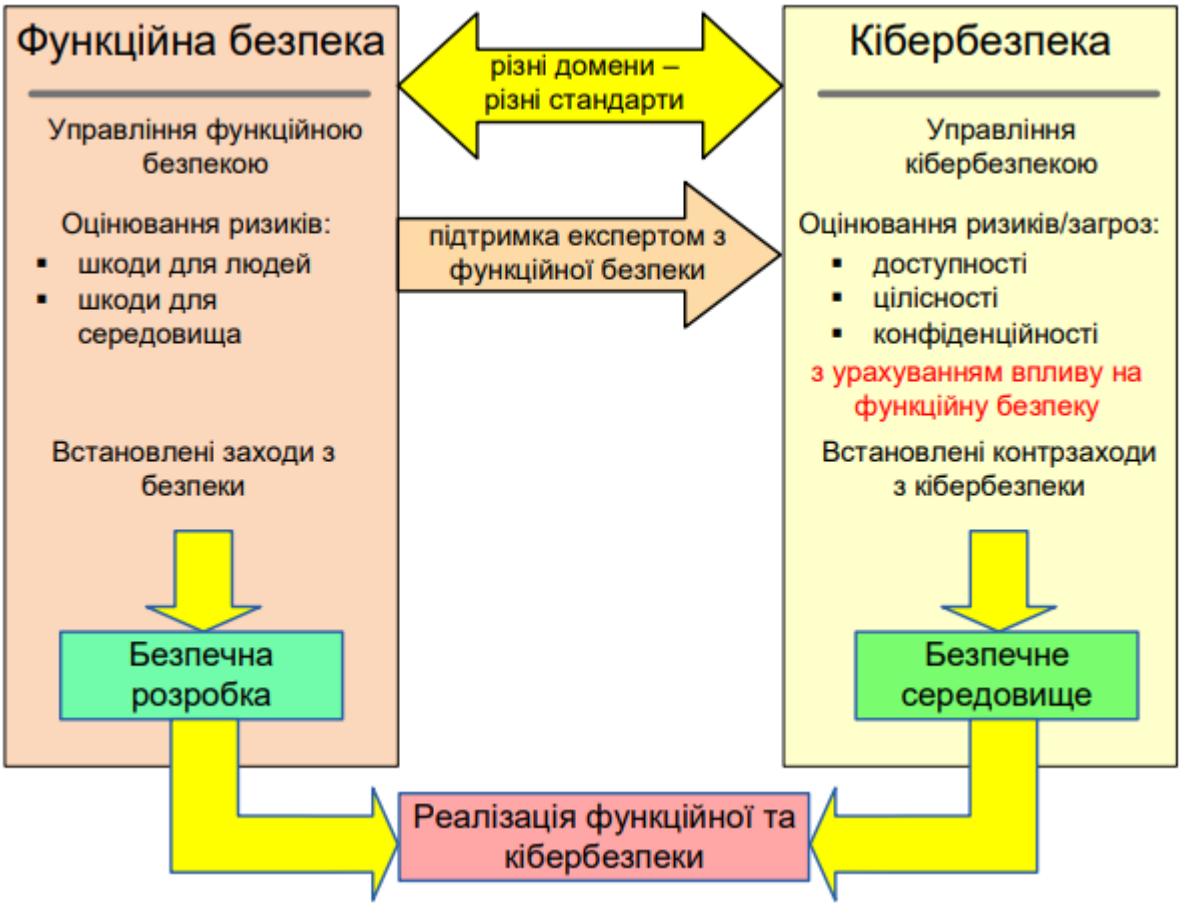

Рисунок 3.4 – Взаємодія функційної безпеки та кібербезпеки.

Функціональним доменом безпеки слід керувати відповідно до IEC 61508 (усі частини).

Доменом мережевої безпеки слід керувати відповідно до IEC 62443 (усі частини).

Управління аспектами функціональної безпеки, пов’язаними з кібербезпекою

При взаємодії між доменом мережевої безпеки та функціональним доменом безпеки, як показано на рис. 3.4, рекомендації полягають у наступному.

1. Аспекти безпеки, пов'язані з функціональною безпекою, повинні керуватися представниками галузі безпеки та досліджуватися під час оцінки загрози безпеці та ризику.

Зауважте, що "керівництво працівниками служби безпеки" не означає, що цим можуть займатись лише експерти з питань безпеки.

2. Потенційний вплив на безпеку, який впливає на функціональну функцію безпеки, повинен бути вирішений за допомогою контрзаходів, визначених для середовища безпеки.

3. Функціональні заходи безпеки та контрзаходи безпечного середовища повинні відповідати керівним принципам для досягнення необхідного зниження ризику в цих двох аспектах.

3.3 Оцінка ризикує

Початковий етап полягає у проведенні заходів з оцінки ризику на більш високому рівні для визначення загального ризику, який потрібно покрити. Оцінку ризику на найвищому рівні можна розуміти як систематичну діяльність, що охоплює два аспекти функціональної безпеки та ідентифікації ризиків та безпеки класифікації.

Оцінка ризику (для функціональної безпеки) та оцінка загроз та ризиків (для безпеки) є подібними процесами, оскільки обидва мають намір врахувати наслідки загроз та / або збоїв. Однак вони в чомусь різні. Наприклад, ймовірність використання вразливостей із розумними загрозами є невизначеною і може бути визначена якісно лише на основі сучасного досвіду. Аспект безпеки не може бути визначений кількісно. Оцінка загрози та ризику кібербезпеки повинна відповідати IEC 62443-2-4, IEC 62443-4-1 та IEC 62443-3-3.

Оцінка функціонального ризику безпеки та оцінка загрози безпеці мережі повинна базуватися на результатах оцінки ризиків вищого рівня.

Незважаючи на те, що дії з оцінки ризиків у сфері функціональної безпеки та безпеки мережі схожі, різниця між ними полягає в тому, що з точки зору функціональної безпеки ймовірність та неімовірнісні причини відмов оцінюються на основі статичних відмов. У той же час поле безпеки мережі оцінює неймовірні причини на основі динамічних сценаріїв уразливості. На цій основі можуть бути встановлені різні процедури та інтервали перегляду. Тому рекомендується застосовувати різні процеси огляду функціональної безпеки та безпеки мережі. Не

існує взаємозв'язку між рівнем цілісності безпеки (SIL) та рівнем безпеки (SL); це слід розглядати як окреме поняття.

Елемент безпеки не є частиною функціональної оцінки ризику безпеки. Вони виділяються в оцінці кібербезпеки, що загрожує. Однак оцінка загроз та ризиків кібербезпеки вимагає співпраці експертів обох галузей.

Під час оцінки загроз та ризиків для безпеки експерти з безпеки та експерти з функціональної безпеки вивчають потенційний вплив на функції функціональної безпеки. Експерт з функціональної безпеки повинен надати детальний опис реалізації функціональної безпеки при впровадженні функціональної безпеки, включаючи перелік активів та відповідні дані (такі як специфікації та конфігурація), що використовуються для побудови системи функціональної безпеки. Експерти з питань безпеки повинні мати можливість зрозуміти прецеденти функціональної безпеки, щоб визначити ризики безпеки, які можуть вплинути на функціональну безпеку.

Коли виявляються конфлікти, слід проводити заходи з вирішення конфліктів. Залежно від організації, вирішення конфліктів може мати різні обов'язки і повинно підтримуватися усіма експертами.

Співвідношення між функціональною безпекою та безпекою промислової автоматизації та системи управління схоже на співвідношення між функціональною безпекою та електромагнітною сумісністю, коли потенційний вплив потрібно оцінити, але загальні норми визначити неможливо.

Інформація про оцінку ризиків вищого рівня повинна надаватися одночасно у сфери функціональної безпеки та безпеки мережі. В обох сферах на основі цієї інформації буде зроблено відповідні оцінки ризиків. Експертам обох галузей потрібно спільно працювати над вирішенням можливих конфліктів та проблем сумісності. Виявлені конфлікти слід вирішувати таким чином, щоб це не впливало на функціональну безпеку та дизайн системи безпеки мережі. На рис. 3.5 показано процес оцінки функціональної безпеки та ризиків мережевої безпеки відповідно до критеріїв IEC61508 та IEC 62443.

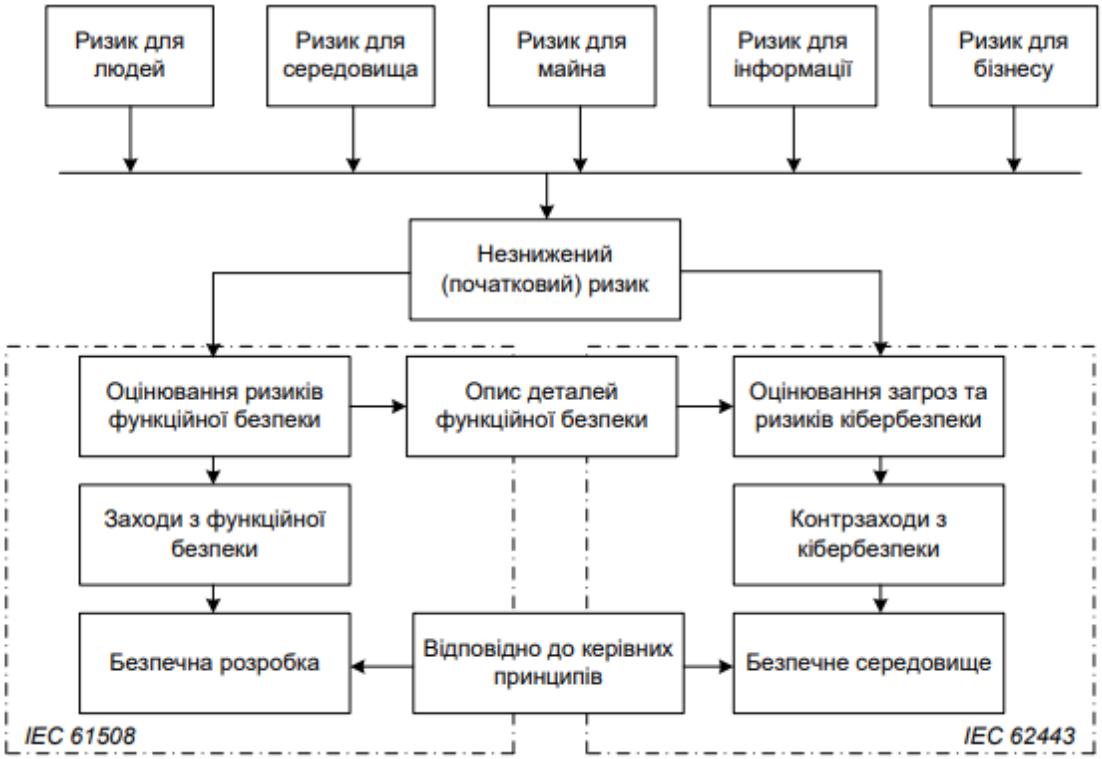

Рисунок 3.5- Оцінювання ризиків

Результати оцінки ризиків найвищого рівня слід використовувати як основу для оцінки ризиків кібербезпеки та оцінки функціональних ризиків безпеки. Через різну природу цих двох аспектів два типи аналізу проводяться окремо. В обох напрямках потрібно визначити заходи щодо зменшення початкового ризику. Процеси, пов'язані з функціональною безпекою або кібербезпекою, можуть виконуватися окремою командою або загальною командою. Експерти з функціональної безпеки та експерти з кібербезпеки повинні прагнути досягти згоди. Якщо угоди немає, слід провести компромісний аналіз.

Взаємозв'язок між функціональною безпекою продукту (у цьому випадку промисловою системою автоматизації та управління) та мережевою безпекою - показано на рис. 3.6. Ліворуч від основних фаз життєвого циклу системи знаходяться заходи, пов'язані з безпекою: система представляє підприємство чи організацію, продукт - промислову систему автоматизації та управління на підприємстві. Праворуч від етапу життєвого циклу знаходяться відповідні норми у галузі функціональної безпеки. Виходячи із встановлених рамок використання, усі

види діяльності з двох областей (функціональна безпека та безпека) пов’язані з певними фазами життєвого циклу.

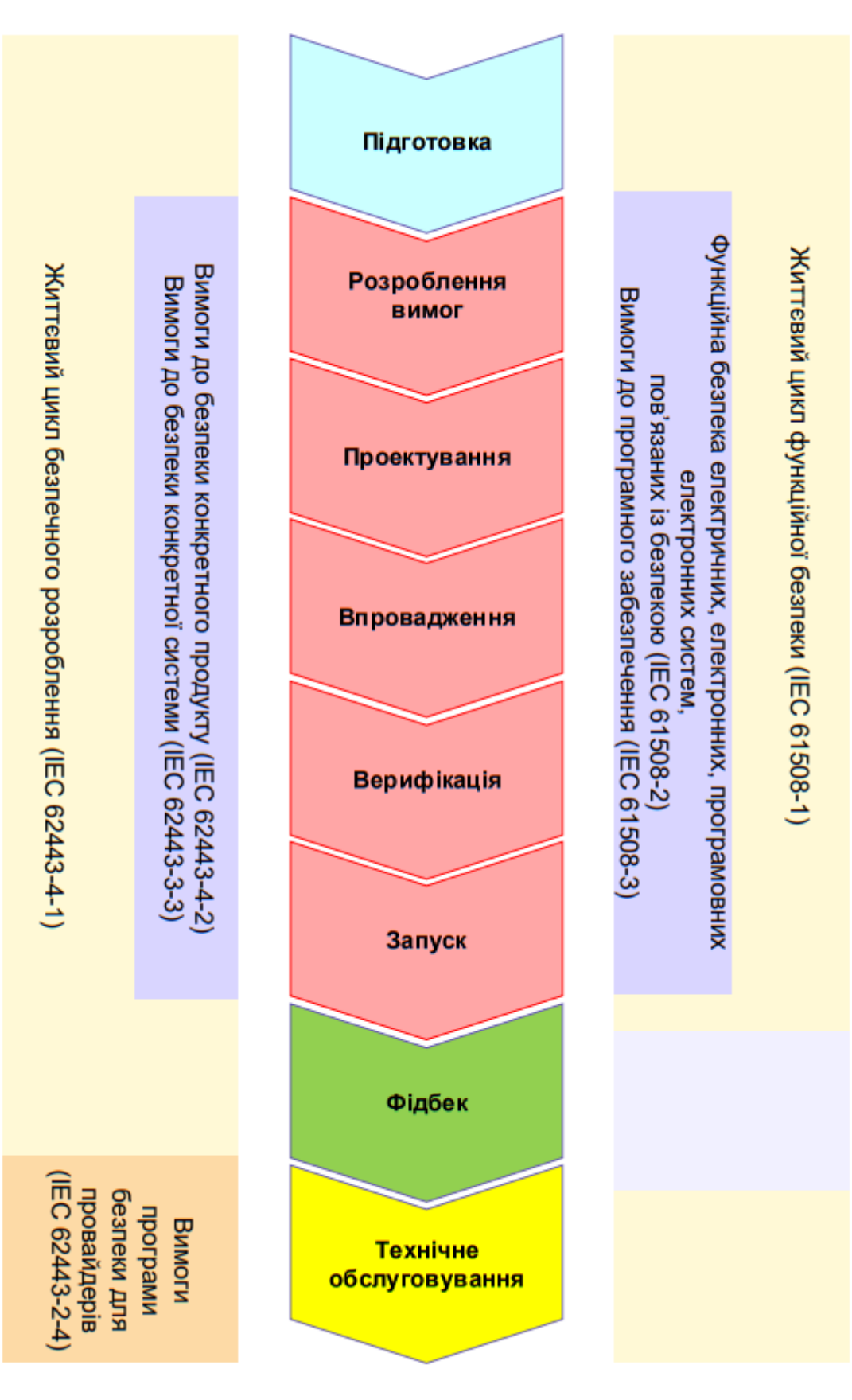

Рисунок 3.6 – Застосування стандартів з безпеки

3.4 Кібербезпека в Україні

На сьогодні законодавство України про кібербезпеку містить багато таких документів, і зв'язок між ними не завжди є чітким та чітким (перераховані в порядку прийняття, що використовується в поточній редакції):

- Закон України «Про оперативно-розшукову діяльність» № 2135-XII від 18.02.1992 р.;
- Закон України «Про Службу безпеки України» № 2229-XII від 25.03.1992 р.;
- Закон України «Про інформацію» № 2658-XII від 02.10.1992 р.;
- Закон України «Про організаційно-правові основи боротьби з організованою злочинністю» № 3341-XII від 30.06.1993 року;
- Закон України «Про державну таємницю» № 3855-XII від 21.01.1994 р.;
- Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» N 80/94-ВР від 05.07.1994 р.;
- Кримінальний кодекс України № 2341-III від 05.04.2001 р.;
- Закон України «Про електронні документи та електронний документообіг» № 851-IV від 22.05.2003 р.;
- Закон України «Про телекомунікації» № 1280-IV від 18.10.2003 р.;
- Закон України «Про ратифікацію Конвенції про кіберзлочинність» N 2824-IV від 07.09.2005 р.;
- Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» № 3475-IV від 23.02.2006 р.;
- Постанова Кабінету Міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» N 373 від 29.03.2006 р.;
- Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010 р.;
- Стратегія національної безпеки України, що затверджена Указом Президента України від 26.05.2015 р. № 287/2015;

- Стратегія кібербезпеки, що затверджена Указом Президента України від 15.03.16 р. № 96/2016 ;
- ДСТУ ISO/IEC 27005:2015 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки;
- ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки;
- Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII від 05.10.2017 р.;
- Закон України «Про національну безпеку України» № 2469-VIII від 21.06.2018 р.;
- Постанова Кабінету Міністрів України «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19 червня 2019 р. № 518.

Короткий аналіз норм кібербезпеки показує їх недоліки та слабкі сторони. Причиною цього є відсутність всеохоплюючої законодавчої бази та наявність певних прогалин та неоднозначностей у самому законодавстві. Важливі такі:

- Необхідність узгодження національного законодавства з міжнародними зобов'язаннями, стандартами та правилами;
- Невідповідність та невідповідність термінології існуючим передовим практикам, міжнародним стандартам та рамкам;
- Необхідність нагляду за кібербезпекою критичних інфраструктур (правила, процедури призначення цілей критичним інфраструктурам, методи оцінки, вимоги до операторів критичної інфраструктури тощо);
- Повторювана юрисдикція на різних рівнях;
- Потреба розробити стратегічний план кібербезпеки, враховуючи обізнаність громадськості про заходи кібербезпеки;
- Заробітна плата державних службовців, що надається для залучення високоякісних фахівців з кібербезпеки, не є конкурентоспроможною;
- Відсутність нормативної підтримки технічного та організаційного нагляду за промисловою автоматизацією та безпекою мереж системи управління.

3.5 Висновки до розділу 3

На даний момент в Україні складно реалізовувати серію IEC 62443

1. Серія IEC 62443 наразі неповна. Деякі технічні характеристики ще не оголошені.

2. Зміст серії IEC 62443 є вичерпним: поточна загальна довжина перевищує 800 сторінок, і очікується, що найближчим часом буде більше специфікацій. Щоб зрозуміти всю серію, потрібно багато часу та зусиль.

3. Вартість отримання повної копії стандарту на офіційному веб-сайті Міжнародної електротехнічної комісії становить понад 2600 доларів США.

4. Стандарти та нормативні документи, як правило, швидко змінюються, тому дуже важливо регулярно їх переглядати та якомога швидше оновлювати національні стандарти. Наприклад, 2020 рік є кінцевим строком для стабілізації наступних норм 62443-1-1, 62443-2-1, 62443-2-3, 62443-2-4 та 62443-3-1.

ВИСНОВКИ

Безпека мережевих та інформаційних систем вважається ключовою проблемою в спробах зберегти функціонування та безпеку цифрової економіки в найближчому майбутньому. В іншому випадку це може мати далекосяжні наслідки для як для економіки і громадян, так і для державного управління. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки розкриваючи принципи цифровізації наголошує, що: «Принцип 7. Цифровізація повинна супроводжуватися підвищенням рівня довіри і безпеки. Інформаційна безпека, кібербезпека, захист персональних даних, недоторканність особистого життя та прав користувачів цифрових технологій, зміцнення та захист довіри у кіберпросторі є, зокрема, передумовами одночасного цифрового розвитку та відповідного попередження, усунення та управління супутніми ризиками».

Окремим напрямком в забезпеченні кібербезпеки цифрової економіки України має стати, поряд з кібербезпекою IT-технологій, кібербезпека операційних технологій (OT- технологій). Продукти і процеси, що охоплюються загальною проблемою кібербезпеки, включають в себе: інформаційні системи, так звані Інформаційної Технології (IT-технології), з необхідністю захисту даних і їх безпечної передачі; фізичні додатки, так звані Операційної Технології - Operations Technology (OT) systems (OT-технології), такі як критично важлива інфраструктура і інтелектуальні системи, і процеси, що забезпечують функціонування цих систем .

Оцінка відповідності кібербезпеки IT та OT технологій відбувається, як правило, за різними стандартами:

• інформаційні системи (Інформаційної Технології - IT) з необхідністю захисту даних і їх безпечної передачі охоплюються, наприклад, оціночними міжнародними стандартами серії ISO/IEC 27000).

• фізичні додатки (Операційної Технології - OT), як правило, охоплюються міжнародними стандартами серії IEC 62443).

Оцінка відповідності – це демонстрація того, що зазначені вимоги виконуються (оцінка відповідності включає такі види діяльності як випробування, інспектування, валідація, верифікація, сертифікація та акредитація). Зазначена вимога (specified requirement) – потреба або сподівання, яке зазначено (зазначені вимоги можуть бути викладені в нормативних документах, таких як регламенти, стандарти та технічні специфікації. Зазначені вимоги можуть бути детальними або загальними).

В роботі було зроблено:

1. Розглянуто системи управління інформаційною безпекою в Україні.
2. Розглянуто серію стандартів IEC 62443 та ISO/IEC 27000.
3. Переглянуто стан кібербезпеки в Україні.
4. Показано, що стан впровадження серії стандарту IEC 62443 на даний момент в Україні досить низький. Через те що Серія IEC 62443 наразі неповна. Деякі технічні характеристики ще не оголошені. Зміст серії IEC 62443 є вичерпним: поточна загальна довжина перевищує 800 сторінок, і очікується, що найближчим часом буде більше специфікацій. Щоб зрозуміти всю серію, потрібно багато часу та зусиль. Вартість отримання повної копії стандарту на офіційному веб-сайті Міжнародної електротехнічної комісії становить понад 2600 доларів США. Стандарти та нормативні документи, як правило, швидко змінюються, тому дуже важливо регулярно їх переглядати та якомога швидше оновлювати національні стандарти. Наприклад, 2020 рік є кінцевим строком для стабілізації наступних норм 62443-1-1, 62443-2-1, 62443-2-3, 62443-2-4 та 62443-3-1.
5. Показано, що правова база України з приводу сертифікації СУІЮ ОТ знаходиться на дуже низькому рівні, що ускладнює сертифікацію ОТ та потребує подальших досліджень.

ПЕРЕЛІК ПОСИЛАНЬ

1. IEC TS 62443-1-1:2009 – Industrial communication networks – Network and system security - Part 1-1: Terminology, concepts and models.
2. IEC 62443-2-1:2010 – Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program.
3. IEC TR 62443-2-3:2015 – Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment.
4. IEC 62443-2-4:2015 – Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers.
5. IEC TR 62443-3-1:2009 – Industrial communication networks – Network and system security - Part 3-1: Security technologies for industrial automation and control systems.
6. IEC 62443-3-3:2013 – Industrial communication networks – Network and system security - Part 3-3: System security requirements and security levels.
7. IEC 62443-4-1:2018 – Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements.
8. IEC 62443-4-2:2019 – Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components.
9. ISO/IEC 27000:2018 – Information technology — Security techniques — Information security management systems — Overview and vocabulary.
10. ISO/IEC 27001:2013 – Information technology- Security techniques- Information security management systems- requirements.
11. ISO/IEC 27002:2013 – Information technology- Security techniques- Code of practice for information security controls.
12. ISO/IEC 27005:2018 – Information technology — Security techniques — Information security risk management.
13. IEC 61508-1, Functional safety of electrical/electronic/programmable electronic safety related systems – Part 1: General requirements.

14. IEC 61508-2, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.

15. IEC 61508-3, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements.

16. IEC 61508-4:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations.

17. IEC 61508-5:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels.

18. IEC 61511 (all parts), Functional safety – Safety instrumented systems for the process industry sector.

19. IEC TR 63069:2019 – Industrial-process measurement, control and automation – Framework for functional safety and security.

20. World Economic Forum. The Global Risks Report 2019 14th Edition.

21. Whitepaper Industrial Security based on IEC 62443, TÜViT Nord Group, 2019.

22. Honeywell Industrial cyber security. Safely embrace the digital age with advanced solutions and services to reduce cyber risk BR-18-4 0-ENG | 09/18.

23. The IACS Cybersecurity Certification Framework. (ICCF). Lessons from the 2017 study of the state of the art, European Reference Network for Critical Infrastructure Protection (ERNCIP Project).

24. Lessons for Operators inIndustrial Cybersecurity eBook 2019, ISA, Siemens.

25. Breaking down cybersecurity and functional safety requirements for industrial control systems, Siemens and CSA Group, 2019.

26. Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications, Schneider Electric, 2018.

27. Effectively Maintaining the Security of Industrial Control Systems, Schneider Electric, 2018.

28. How to Effectively Implement ISA 99 / IEC 62443, Forescout, 2019.

29. Establishing zones and conduits industrial cybersecurity center In accordance with the ISA99/IEC 62443 standard, ICC. 2018.

30. Process Control Networks Secure Architecture Design, Honeywell, 2012

31. Industrial cyber security. Safely embrace the digital age with advanced solutions and services to reduce cyber risk. Honeywell, 2018.

32. Technical guide Cybersecurity for ABB drives, ABB, 2017.

33. Define your functional safety and cyber security requirements to optimise safety & security, ABB, 2019.

34. U.S. Department of Energy Cybersecurity strategy 2018-2020.

35. Правова база української кібербезпеки: загальний огляд і аналіз, Міжнародна фундація виборчих систем, 2019.

36. Навчальні матеріали проекту “Модернізація курсів з інформаційної безпеки та стійкості” / Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains SEREIN https://serein.eu.org/

37. Навчальні матеріали проекту “Інтернет речей: нова навчальна програма для потреб промисловості та суспільства” /Internet of Things: Emerging Curriculum for Industry and Human Applications ALIOT https://aliot.eu.org/

38. Tsvilii O. CYBERSECURITY REGULATION: CYBERSECURITY CERTIFICATION OF OPERATIONAL TECHNOLOGIES. Аудит технологій та виробничі резерви, 2021, pages 54–60.